NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ENHANCED CYBERSPACE DEFENSE WITH REAL-TIME DISTRIBUTED SYSTEMS USING COVERT CHANNEL PUBLISH-SUBSCRIBE BROKER PATTERN COMMUNICATIONS

by

Steven G. B. Paxton

June 2008

Thesis Advisor: James B. Michael
Second Reader: George W. Dinolt

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Enhanced Cyberspace Defense through Covert Publish-Subscribe Broker Pattern Communications		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Major Steven G. B. Paxton			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

In this thesis, we propose a novel cyberspace defense solution to the growing sophistication of threats facing networks within the Department of Defense. Current network defense strategies, including traditional intrusion detection and firewall-based perimeter defenses, are ineffective against increasingly sophisticated social engineering attacks such as spear-phishing which exploit individuals with targeted information. These asymmetric attacks are able to bypass current network defense technologies allowing adversaries extended and often unrestricted access to portions of the enterprise. Network defense strategies are hampered by solutions favoring network-centric designs which disregard the security requirements of the specific data and information on the networks. Our solution leverages specific technology characteristics from traditional network defense systems and real-time distributed systems using publish-subscribe broker patterns to form the foundation of a full-spectrum cyber operations capability. Building on this foundation, we present the addition of covert channel communications within the distributed systems framework to protect sensitive Command and Control and Battle Management messaging from adversary intercept and exploitation. Through this combined approach, DoD and Service network defense professionals will be able to meet sophisticated cyberspace threats head-on while simultaneously protecting the data and information critical to warfighting Commands, Services and Agencies.

14. SUBJECT TERMS Cyberspace, Cyberspace Defense, Network Defense, Distributed Systems, Covert Channel Communications			**15. NUMBER OF PAGES** 115
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ENHANCED CYBERSPACE DEFENSE WITH REAL-TIME DISTRIBUTED SYSTEMS USING COVERT CHANNEL PUBLISH-SUBSCRIBE BROKER PATTERN COMMUNICATIONS

Steven G. B. Paxton
Major, United States Air Force
B.S., Chapman University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Author: Major Steven G. B. Paxton

Approved by: Professor James B. Michael
Thesis Advisor

Professor George W. Dinolt
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this thesis, we propose a novel cyberspace defense solution to the growing sophistication of threats facing networks within the Department of Defense. Current network defense strategies, including traditional intrusion detection and firewall-based perimeter defenses, are ineffective against increasingly sophisticated social engineering attacks such as spear-phishing which exploit individuals with targeted information. These asymmetric attacks are able to bypass current network defense technologies allowing adversaries extended and often unrestricted access to portions of the enterprise. Network defense strategies are hampered by solutions favoring network-centric designs which disregard the security requirements of the specific data and information on the networks. Our solution leverages specific technology characteristics from traditional network defense systems and real-time distributed systems using publish-subscribe broker patterns to form the foundation of a full-spectrum cyber operations capability. Building on this foundation, we present the addition of covert channel communications within the distributed systems framework to protect sensitive Command and Control and Battle Management messaging from adversary intercept and exploitation. Through this combined approach, DoD and Service network defense professionals will be able to meet sophisticated cyberspace threats head-on while simultaneously protecting the data and information critical to warfighting Commands, Services and Agencies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BACKGROUND....2
1. The State of Cyberspace Defense....2
2. Real-Time Distributed Systems....2
3. Covert Channel Communications....3
4. Case Study: The Cyber Operations and Information System....3
B. OBJECTIVE: A PROPOSAL FOR A FULL-SPECTRUM DATA-CENTRIC CYBERSPACE DEFENSE SYSTEM....3
1. Sub-Objective One: Recognize that Current Network Defense Strategies are Inadequate....3
2. Sub-Objective Two: Recognize that Future Network Defense and Cyberspace Defense Systems must Focus on Information-Centric Distributed Systems versus Network-Centric Client-Server Designs....4
3. Sub-Objective Three: Recognize that Critical C2 and Battle Management (BM) Communications in a Network Defense Environment must be Protected from Adversary Interception....4

II. THE STATE OF CYBER DEFENSE....5
A. INTRODUCTION....5
B. NETWORK VULNERABILITIES....6
1. Network Security is not a New Concept....6
2. Phishing: The User as an Unwitting Accomplice....7
3. The Link between Phishing and Botnets....8
4. Spear-Phishing....9
C. THE ADVERSARY IS ALREADY ON OUR NETWORK – AND IS HERE TO STAY....10
1. Organized Persistent Network Intrusions....10
a. Case 1....10
b. Case 2....11
2. Threats to Critical Infrastructure....11
3. The Chinese Threat....12
4. Threat Assessment from the Director of National Intelligence....13
D. NETWORK VULNERABILITIES ARE INCREASING....14
1. Complexity of the GIG....14
2. Sacrificing Security for the Sake of Being Inter-connected....16
3. Network-Centric Warfare (NCW)....17
4. The Host-Based Security System (HBSS)....18
E. A DIFFERENT APPROACH TO CYBERSPACE DEFENSE....22
1. Cannot "Plug the Dyke"....22
2. Proposed Solutions....23
a. Intrusion Detection Systems....23
b. Future Technology-based Network Defense Solutions....24

c. Network Defense as a National Strategy 25
d. Incident Response 26
F. CONCLUSION 30

III. REAL-TIME DISTRIBUTED SYSTEMS 33
A. DISTRIBUTED COMPUTING 33
1. Distributed Intrusion Detection 34
2. Intrusion Tolerance 36
B. REAL-TIME COMPUTING 37
C. REAL-TIME DISTRIBUTED COMPUTING SYSTEMS AND STANDARDS 40
1. Client-Server 40
2. Message Passing 41
3. Publish-Subscribe 41
a. Topic-based Publish-Subscribe 42
b. Content-based Publish-Subscribe 42
c. Type-based Publish-Subscribe 42
4. Publish-Subscribe for Cyberspace Defense 43
5. Object Management Group's Data Distribution Service for Real-Time Systems (DDS) 44
6. DDS and Distributed Cyberspace Defense 46
a. Complex Data Flow 46
b. Latency Requirements 46
c. Large Networks 47
d. High Data Rates 47
e. No Single Point of Failure 47
f. Self-healing Communication and Dynamic Configuration 48
g. Quality of Service 48
h. Discovery 50
7. Real-Time Innovations DDS 50
8. OpenSplice DDS from PrismTech 51
D. CONCLUSION 54

IV. COVERT CHANNEL COMMUNICATIONS 55
A. COVERT CHANNELS DEFINED 57
B. NETWORK BASED COVERT CHANNEL IMPLEMENTATIONS 62
1. Addressing Channel 63
2. Data Block Length Channel 63
3. IP Fragmentation Channel 64
4. Steganography in Networking using Toral Automorphism 64
5. Protocol Hopping Covert Channel 65
C. COVERT CHANNELS IN DISTRIBUTED SYSTEMS 65
1. ACK Channel 65
2. DBMS Channel 66
D. CONCLUSION 66
1. Further Reading on Covert Channels 67

V. CASE STUDY – CYBER OPERATIONS INFORMATION SYSTEMS 69
A. COIS BACKGROUND 69
1. Purpose of the System.....70
a. Cyber Defense Strategy Problems 71
b. Cyber Defense Awareness Problems 71
c. Cyber Defense Knowledge Problems.....72
d. Cyber Defense Organizational Problems 72
B. COIS OVERVIEW 73
1. Virtual Cell Organizational Model.....73
a. Virtual Cell Members.....75
b. Core Communities.....75
2. Architecture.....78
C. INTEGRATION OF COVERT CHANNELS.....80
VI. CONCLUSION 83
A. SUMMARY 83
B. STRATEGIC RECOMMENDATIONS FOR NEXT GENERATION CYBERSPACE DEFENSE 86
1. Traditional Network Defense Capabilities 87
2. Real-Time Distributed Systems 87
3. Covert Channel Broker Pattern Technology 88
C. AREAS OF FUTURE RESEARCH.....88
1. Cyberspace and Network Defense.....88
2. Real-Time Distributed Systems 89
3. Covert Channels and Information Protection.....89
LIST OF REFERENCES.....91
INITIAL DISTRIBUTION LIST 99

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1 - U.S. CERT Top Five Incidents vs. All Others From [10] 8
Figure 2 - The Network-Centric GIG From [20] 15
Figure 3 - DoD McAfee-based HBSS System From [25] 20
Figure 4 - Domestic and International Computer Incident Response 28
Figure 5 - National FIRST Organizations 29
Figure 6 - Client-Server Based Distributed Systems From [45] 33
Figure 7 - Firewall Errors versus Firewall Rule Complexity From [60] 39
Figure 8 - OMG DDS Publish-Subscribe Model From [64] 44
Figure 9 - Use of Topics in DDS Publisher-Subscribe Middleware From [65] 45
Figure 10 - DDS Subscription Matching with QoS and Type Information From [68] 50
Figure 11 - RTI DDS Decentralized Architecture From [69] 51
Figure 12 - OpenSplice DDS Federated Architecture From [69] 52
Figure 13 - OpenSplice Shared Memory Data Space From [68] 53
Figure 14 - Plaintext Message Exchange 55
Figure 15 - Encrypted Message Exchange 56
Figure 16 - Covert Message Exchange 57
Figure 17 - COIS Virtual Cells versus Physical Cells From [96] 74
Figure 18 - COIS Dynamic Communities From [96] 77
Figure 19 - COIS Architecture From [96] 78
Figure 20 - COIS Strategic Operational Model with Mobile Agents From [96] 79
Figure 21 - Traditional versus Virtual Vulnerabilities After [96] 81
Figure 22 - Full-Spectrum Cyberspace Defense Characteristics 87

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author would like to humbly thank Professors Brett Michael and George Dinolt for their patience and support during the research and writing of this thesis as well as their dialog, enthusiasm and passion for the subject of cyberspace defense which was the initial inspiration for embarking on this important journey. Additional thanks to Mr. John Sarkesain of the Missile Defense Agency for his support and feedback regarding the COIS program without which, this thesis would not have been possible. And lastly, many thanks for the comments and unrestrained dialog from Major Ben Hinton and Major Kevin Yates which proved invaluable to ensure this thesis stayed relevant and operationally focused

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> *I used to think that cyberspace was fifty years away. What I thought was fifty years away, was only ten years away. And what I thought was ten years away... it was already here. I just wasn't aware of it yet.*
>
> *Bruce Sterling, 1993 [1]*

These words illustrate the dilemma facing technologists, engineers, scholars and even the military and are as relevant today as they were in 1993. They highlight a fundamental misunderstanding, misperception and even miscalculation of what cyberspace is and how to operate within its limits. But more importantly, they capture the daily struggle to understand how to defend cyberspace.

> *This is just the beginning; the beginning of understanding that cyberspace has no limits, no boundaries.*
>
> *Nicholas Negroponte, 1999 [2]*

Affirmation from Mr. Negroponte came when he was speaking to an Internet group about the concept of time in cyberspace; a place with no borders and essentially no limits. He spoke these words in 1999 and yet our evolved understanding and recognition of cyberspace in the macro view as a limitless domain of networks, never followed. We continued to hobble down a path of monolithic network-centric solutions and strategies, funding network security versus cyberspace security, approaching network defense as a network problem versus an information problem.

While ultimately solving "the problem of cyberspace defense" is beyond the scope of this thesis, we present a solution to defending our portion of cyberspace, not as a network, but as information which needs to be protected; information-centric versus network-centric defense.

The purpose of this thesis is, therefore, to propose a structured, information-centric, distributed network system employing covert channel publish-subscribe broker pattern communications to improve the protect-detect-react cycle of defending systems in cyberspace.

A. BACKGROUND

This thesis is organized into three main chapters which focus on the underlying principles or objectives of the overall proposal; network defense, distributed systems, and covert channel communications. Following the main body of the thesis, we devote a fourth chapter to a case study which highlights that this goal is realistic and attainable.

1. The State of Cyberspace Defense

Chapter II focuses on several complex issues that lay the foundation for a new approach to network security which is fraught with numerous challenges. This chapter begins with a brief discussion of the history of network security and that while not a new subject, the numbers and types of threats are constantly changing, creating an extremely difficult environment to protect. We then look at several examples of how attacks can be used by an adversary to gain control of a host or network and gather vital intelligence or steal data without detection.

A solution is proposed at the end of this chapter and expanded in later chapters addressing the need for security professionals to rapidly respond to events and attacks throughout their own enterprise, often to multiple simultaneous events at multiple security and access levels, while collaborating with other teams to ensure adequate information sharing.

2. Real-Time Distributed Systems

Chapter III introduces a software architecture that is well suited for a cyberspace defense system known as real-time distributed middleware.

Distributed and real-time computing concepts are discussed in the context of intrusion detection, network security and cyberspace defense and how each contributes to various networking requirements, and when combined, present an extremely desirable set of technology characteristics for cyberspace defense.

Under the context of integrated real-time software design solutions, a discussion of middleware is presented, outlining the three major categories of real-time designs: client-server, message passing and publish-subscribe.

3. Covert Channel Communications

Chapter IV introduces covert channel technology and how this unique method of communication can be applied in a distributed real-time cyberspace defense system.

Our discussion of covert channels is from the standpoint that information communicated between users of a networked system must be protected from adversary detection. In many cases, simply the presence of communication, or the ability to monitor important message traffic, is more valuable to the adversary than mining data from the network. This information can reveal forensic and network defense tactics, techniques and procedures that, while not classified, should be protected to the maximum extent possible.

4. Case Study: The Cyber Operations and Information System

In order to propose a solution for a full-spectrum command and control and battle management cyberspace defense capability, an evaluation of traditional network defense technology, real-time distributed system technology as well as covert channel technology was performed.

This program presented in Chapter V brings two areas together; network defense and real-time distributed systems technology which effectively represent a near complete solution. We present the main features of this program and conclude with a proposed strategy to integrate the missing piece; covert channel communications.

B. OBJECTIVE: A PROPOSAL FOR A FULL-SPECTRUM DATA-CENTRIC CYBERSPACE DEFENSE SYSTEM

In order to achieve the stated objective in a logical and methodical fashion, we will breakdown the analysis into three sub-objectives to provide clarification and detail.

1. Sub-Objective One: Recognize that Current Network Defense Strategies are Inadequate

The first sub-objective, detailed in Chapter II, is to provide an in-depth analysis of current trends in cyber-space with an acknowledgment that current technological

solutions are ineffective and inappropriately organized against the growing threat to enterprise networks and cyber-space in particular.

2. Sub-Objective Two: Recognize that Future Network Defense and Cyberspace Defense Systems must Focus on Information-Centric Distributed Systems versus Network-Centric Client-Server Designs

The second sub-objective, detailed in Chapter III, is to provide a proposed solution to the architectural challenges raised by Chapter II. In other words, recognizing that traditional network-centric cyber-defense solutions, the focus of current and future DoD network defense, are inadequate and inappropriately organized, what technology is the most effective or better suited? We propose an information-centric distributed system model incorporating open standard publish-subscribe middleware as a foundation for developing a full-spectrum cyberspace defense and C2 capability.

3. Sub-Objective Three: Recognize that Critical C2 and Battle Management (BM) Communications in a Network Defense Environment must be Protected from Adversary Interception

The third sub-objective, detailed in Chapter IV, is to provide an analysis of covert channel communication theories and technology and propose a methodology whereby critical communication within a cyber-defense system is protected from adversary interception, maintaining security and integrity of operational capabilities of the organization and its mission.

II. THE STATE OF CYBER DEFENSE

The great uncertainty of all data in war is a peculiar difficulty, because all action must, to a certain extent, be planned in a mere twilight, which in addition not infrequently — like the effect of a fog or moonshine — gives to things exaggerated dimensions and unnatural appearance.

Carl von Clausewitz [3]

A. INTRODUCTION

This chapter focuses on several complex issues that lay the foundation for a new approach to network security which is fraught with uncertainty and complexity. As Clausewitz points out, warfare, at its very core, deals with uncertainty. It is imperative therefore that network defense consider the uncertainty of cyberspace, to address and overcome both threats in cyberspace, and the cyber "fog of war."

We begin with a brief discussion of the history of network security and that while not a new subject, the numbers and types of threats are constantly changing, creating an extremely difficult environment to protect. We then look at several examples of how specific attacks can be used by an adversary to gain control of a host or network and gather vital intelligence or steal data without detection. A critical conclusion from these examples is that the enemy has had a long presence on the specific networks and has amassed a great deal of information about the network he uses to avoid detection for as long as possible.

A large part of the problem with respect to network security is not that there is a threat on the networks. Rather, it is that network strategists have adopted a sense of interoperability and information sharing which provide unprecedented levels of access to all network users. The reality that this dilemma poses is that networks are growing increasingly complicated and interconnected.

Another problem facing network defense strategists in both the public and private sector is that of terminology. That is, how is network defense different from cyberspace

defense? For the purposes of this thesis, we treat network defense (Net D) as a subset of cyberspace defense. For example, a university network that has its own security policies and security appliances is practicing network defense. Cyberspace was recently defined by the National Military Strategy to Secure Cyberspace as: "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures [4]." In the context of information technology, a *computer network* is broadly defined as: a system of computers, peripherals, terminals and databases connected by communications lines [5]." We can add that a computer network is typically organized for a specific purpose (i.e., a university network, or a business network, etc.) Cyberspace, as the National Strategy indicates, is inclusive of all electronics, the entire electromagnetic spectrum and networked systems. Thus computer network defense (Net D) is a subset of cyberspace defense.

B. NETWORK VULNERABILITIES

1. Network Security is not a New Concept

The need to protect computers and networks of computer systems is not new. One of the earliest reports acknowledging the need to address computer security was commissioned as a result of a 1967 Advanced Research Projects Agency Task Force to study and recommend computer security safeguards in order to protect classified information. The now famous "Ware Report", published in 1970 is considered the first documented requirement to formally define computer security, and the measures necessary to ensure information and computer systems remain protected. In capturing the essence of his charter, Ware stated:

> *A basic principle underlying the security of computer systems has traditionally been that of isolation--simply removing the entire system to a physical environment in which penetrability is acceptably minimized. The increasing use of systems in which some equipment components, such as user access terminals, are widely spread geographically has introduced new complexities and issues. These problems are not amenable to solution through the elementary safeguard of physical isolation [6].*

That the researchers and authors of this report had the foresight to recognize the growing use of interconnected resources is outstanding. However, the fact that we are still struggling with the security implications first identified in 1970 is troublesome.

2. Phishing: The User as an Unwitting Accomplice

Social engineering bypasses all technologies, including firewalls.

Kevin Mitnick [7]

One of the most insidious examples of breeching network defenses is the relatively recent trend of phishing. In the most common usage, phishing is associated with the release of email spam for the purposes of harvesting personal information to facilitate identity theft or to release trojan malware to gain access to the network. According to the Anti-Phishing Working Group (APWG), the practice of phishing as well as the term used to describe it dates back to 1996 when AOL accounts were stolen by sending email that appeared to originate from AOL, to users requesting their personal information [8].

The U.K. based Millersmiles.com, which tracks online phishing scams has a current database of 675 public companies that are, or have been, the target of a total of nearly 400,000 separate incidents [9]. Additionally, the U.S. Computer Emergency Response Team (CERT) lists phishing as the number one type of incident reported in the second quarter of 2008 where 72.5% of all incidents during that timeframe were phishing incidents (Figure 1) a dramatic increase from the first quarter report of 45% in February 2008 [10].

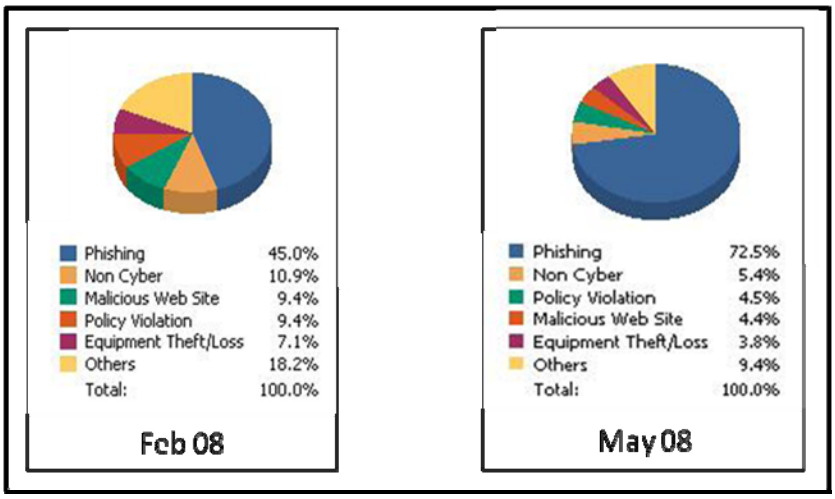


Figure 1 - U.S. CERT Top Five Incidents vs. All Others From [10]

While phishing attacks are typically associated with spam email, identity theft, credit card scams and in some cases with denial of service (DOS) attacks, it wasn't until recently that the connection between well organized armies of computers under unified control and phishing scams was known.

3. The Link between Phishing and Botnets

The FBI has recently reported the connection of phishing emails, or unsolicited emails that suspiciously request users click unknown links or provide personal information, with the growing threat from botnets [11]. Botnets (or roBOT NETworkS) are the legions of computers running malware that allows a botnet herder to control the botnet for the purposes of sending out more spam (to collect more bots for the net), or to act as relays during Distributed Denial of Service attacks. This application of phishing represents one broad-based use from the criminal element.

In fact, Botnets have shown promise in criminal circles as being extremely versatile by storing large amounts of stolen personal information and by being the launch point for Distributed Denial of Service (DDoS) attacks and for sending spam which clogs our inboxes.

One innovative solution proposed by Williamson [12], suggests developing a government controlled botnet to protect against adversary DDoS attacks. This capability would require a central control authority that could command and control the botnet to maximize effectiveness while minimizing collateral damage. While provocative and guaranteed to illicit discussions about cyberspace operations and non-kinetic warfare, controlling a botnet with the degree of precision necessary to avoid unintended collateral damage or second and third order effects would be unrealistic. Further, the potential for an adversary to hijack a U.S. military botnet and use it against our own, or coalition, forces would unnecessarily risk national policy and world opinion.

4. Spear-Phishing

Spear-phishing is a variation of the phishing scam which incorporates a more tailored approach to exploiting network defenses. The SANS Institute describes spear-phishing as, "a highly targeted phishing attack." [13] Spear-phishing methodology differs from normal phishing emails in that whereas a normal phishing email relies on large numbers of the same email message being released by a botnet or other spam relay, a spear-phishing attack, specifically targets a small group of people in one company, or even a specific individual by using familiar references in the email, in hopes of gaining their trust to click on a link or provide personal information. In fact, that is precisely where the traditional mind-set of network defense and cyber-security has failed since the Ware Report first identified the problems of network security in 1970; defense against social networking attacks.

Phishing and spear-phishing represent a type of threat that traditional network defense has been unsuccessful at thwarting. This is due to the fact that the social-engineering required to convince the intended target that the email is real, is so well executed, and so well researched that most users are not aware that they have become unwitting accomplices in the impending attack or identity theft. While most intrusion detection and prevention systems are able to detect the presence of malware based hard coded scripts (Java, Visual Basic, etc.) a hyper-link is typically not scanned due to resource and technological constraints required to track links back to their referring site

and determine the site's intent. Additionally, verifying and authenticating the identity of the sender is an extremely difficult challenge given the availability of anonymizers and other botnet obfuscation tools available on the internet.

C. THE ADVERSARY IS ALREADY ON OUR NETWORK – AND IS HERE TO STAY

Never underestimate the time, expense, and effort an opponent will expend to break a code.

Robert Morris, Retired NSA Scientist, 1995 [14]

1. Organized Persistent Network Intrusions

In December 2007, Dr. Ron Ritchey of Booz|Allan|Hamilton, presented a sobering picture of what happens when a well organized attacker is able to leverage the access gained from a spear-phishing attack [15]. In his presentation, he outlined two cases of prominent organizations with security policies that were the subject of repeated and prolonged network attacks. What is most striking about these two incidents is not simply that they occurred, but the level of sophistication with which they were executed by the attackers and by the obvious doctrine and tactics, techniques and procedures (TTP) that were employed during the attacks.

a. Case 1

The forensic analysis provided by Dr. Ritchey's team revealed that the attackers were choosing their targets with skill and much care, and that the network had been compromised for months. Key points from his analysis of this case:

- Client executives and key employees have been attacked with highly targeted and sophisticated spear-phishing attacks

- The attackers are collecting data from key technical users

- The attackers appear to focus on the target's defense-related sites

- The target's corporate network has been fully compromised at least since Mar 2007, although the attackers probably have been on the network for much longer

Dr. Ritchey's analysis further identified that the attackers were able to re-compromise several systems just hours after malicious code had been eradicated from them. Additionally, the attackers were using extreme caution and were utilizing countermeasures to prevent the analysis team from identifying the malicious code being employed [15].

b. Case 2

The second example involved a major corporation with over 100,000 employees and a strong security program. Despite their vulnerability assessments and scanning, firewalls, network and host-based IDS, and a well-trained security team, their systems were compromised as much as with the first example. Dr. Ritchey's team discovered that keyloggers were widely deployed allowing the attackers to profile and perform long-term intelligence gathering on specific employees and the overall organization [15].

Clearly these two cases represent a much more than a relatively simple case of identity theft. What is important to understand is that the initial vector to achieve access to the network in Dr. Ritchey's examples and the ability to phish for personal credit card information against a private citizen is the same. The weakness is in the psychological vulnerability of the network, i.e., the person behind the keyboard. The dangerous link in these two examples is that knowing which person to target and then exploiting that person can, and in many cases, allow access to deeper enclaves within the enterprise network. While the protection of data from exfiltration, corruption or deletion is a major concern for many network defense strategists, some of these networks and systems are more than just data repositories.

2. Threats to Critical Infrastructure

Supervisory Control and Data Acquisition (SCADA) systems represent one of the major concerns for many in government and private sectors and an area that must be

addressed by DoD cyberspace defense strategists. As with traditional enterprise networks such as corporate or military information technology, SCADA systems exist as a subset of cyberspace. In other words, they are interconnected. Just as the Federal Government's level of interconnectedness is growing, so is the information sharing throughout the various sectors of the U.S. infrastructure such as power, transportation and water.

In fact, the National Strategy to Secure Cyberspace lists "Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States" as one of its top responsibilities [16]. While this document was published in Feb 2003, nearly five years later, security experts are publishing results that SCADA systems which run and regulate the nations utility and critical infrastructure systems are increasingly vulnerable due to increased access and information sharing programs [17].

3. The Chinese Threat

There is probably no greater potential threat to the U.S. information infrastructure, and arguably all of cyberspace, than the People's Republic of China. Examples of Chinese incursions into networks across the globe are released daily and are the subject of intense scrutiny and study to determine precise attribution (whether they are in fact state sponsored, or simply rogue elements within the PRC) doctrine and intent. In Secretary of Defense's 2008 report on the growing Chinese cyber warfare capabilities, it states [18].

In the past year, numerous computer networks around the world, including those owned by the U.S. Government, were subject to intrusions that appear to have originated within the PRC. These intrusions require many of the skills and capabilities that would also be required for computer network attack. Although it is unclear if these intrusions were conducted by, or with the endorsement of, the People's Liberation Army (PLA) or other elements of the PRC government, developing computer network attack capabilities is consistent with authoritative PLA writings on this subject [18].

In line with the examples of highly organized intrusions provided by Dr. Ritchey, the Secretary of Defense's report further states: "In 2007, the DoD, other U.S. Government agencies and department and defense-related think tanks and contractors experienced multiple computer network intrusions, many of which appeared to have originated in the PRC [18]." This statement confirms that not only are DoD networks a target for foreign governments like the PRC, but that they are vulnerable and exploitable. Regrettably, the DoDs vulnerability is compounded by the trend of interconnecting between agencies and information sharing at the federal, state and local levels following the events of September 11, 2001.

4. Threat Assessment from the Director of National Intelligence

The Director of National Intelligence's (DNI) Information Sharing Environment (ISE) is one example where the isolation of networks prevented the possible fusion of information which some contend could have helped to mitigate some of the precursor events to 9/11. The unintended consequence of information sharing and interoperability initiatives, particularly at the scope of the DNI's ISE, raises the stakes of risk and cyber warfare to a national level and ultimately a national problem. Acknowledging this cyber risk to the nations infrastructure, the DNI, Mr. Michael McConnell, recently gave his Annual Threat Assessment before the Hearing of the Senate Armed Services Committee. During this 27 Feb, 2008 statement, Mr. McConnell stated:

> *The United States information infrastructure, including telecommunications and computer networks and systems, and most importantly the data that resides on these systems is critical to virtually every aspect of our modern life. Threats to our intelligence infrastructure are an important focus of this community. We assess that nation-states – which include of course, Russia and China – long have had the technical capability to target U.S. information systems for intelligence collection.*
>
> *Today, those countries and others could target our information infrastructure for data degradation or data destruction. Data destruction as opposed to data exploitation is of increasing concern because of the potential impact on U.S. and the global economy should such perpetrators be successful [19].*

The HASC Chairman, Senator Thune (D-MI) later asked Mr. McConnell what type of cyberspace threat he viewed as the most dangerous; and is DNI prepared to deal with those threats from either a civil or military aspect. To which Mr. McConnell simply stated:

> *Sir, we're not prepared to deal with it* [19].

Mr. McConnell continues by saying:

> *…our worry right now is the military's probably the best protected. The federal government is not well-protected and the private sector is not well-protected. So the question is, how do we take some of the things that we've developed for the military side, scale them across the federal government. And the key question will be, how do we interact with the private sector? [19]*

D. NETWORK VULNERABILITIES ARE INCREASING

1. Complexity of the GIG

As networks and technology becomes more complex, as the number of lines of code written to implement this new, complex technology increases by orders of magnitude, and as the interconnectedness of corporate and enterprise networks increase to the point where there is no real physical distinction between different domains, the defense of those computers and networks becomes equally complex, challenging and often mired in the same technology intended to protect the same networks.

The 2007 Global Information Grid (GIG) Architectural Vision highlights the increasing complexity that military Cyberspace leaders are confronted with [20]. As Figure 2 conveys the network-centric GIG is based on a myriad connections throughout the GIG architecture to maximize information sharing and interoperability. The advantage to this type of architecture is the availability and access to numerous types of information.

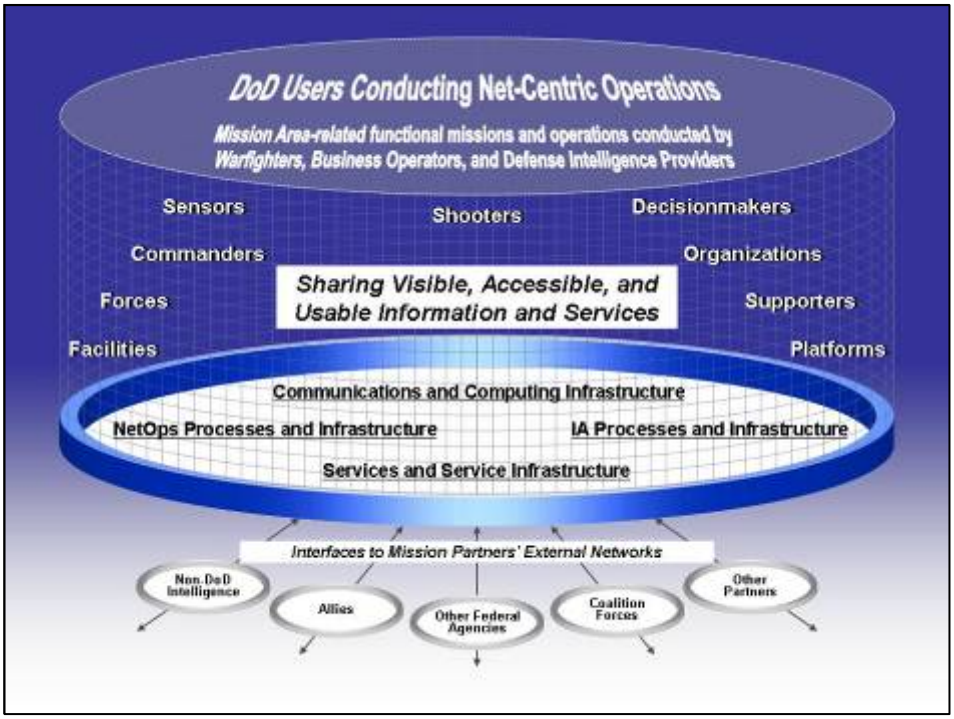


Figure 2 - The Network-Centric GIG From [20]

The disadvantage to this type of architecture, however, is that there are too many connections and too many networks over which to realistically maintain control. At the bottom of Figure 2, the interfaces identified in the Vision document clearly indicate the numerous connection points that make a unified network defense strategy challenging; non-DoD Intelligence, Allied and Coalition network interfaces, other Federal Agencies which do not have strict network policy management or enforcement, and "other Partners". Each of these entities has their own security policies and priorities which may or may not be compatible with our own. Each has different levels of funding which manifest in varying types of technology solutions, again which may or may not be compatible with our own. Despite these differences and challenges, the task remains to interconnect and share information to the extent possible, ostensibly to improve our operational capability, efficiency and security. However, this charter seems in direct conflict with our ability to protect and defend that same "open" architecture.

2. Sacrificing Security for the Sake of Being Inter-connected

The quest for increasing interconnectedness becomes even more of a network security liability when other critical infrastructure applications and networks are factored into the enterprise defense strategy.

Large-scale infrastructures that provide nationwide mission-critical services are usually managed (or at least regulated) by a national central authority. An example is the U.S. National Power Grid [21]. Thus mission critical networks must survive and interoperate within an un-trusted heterogeneous environment [21]. The implications of this model suggest that protection must rely on "local surveillance" and "global coordination and control".

Local protection addresses the boundary protection and hardening of local network infrastructure but does not address the external threats that are increasingly the threat (i.e., Distributed Denial of Service attacks, phishing, pharming[1], etc.)

The future threats to the infrastructure will involve numerous protection domains as victims or unwilling collaborators. There is a need, therefore, to create a nationwide security infrastructure that enables the correlation of security-related information coming from different subsystems to obtain a global view of the security state of the infrastructure and that enables command and control capabilities from a central or distributed control station [21].

The ability to integrate the information coming from different parts of the network, to coordinate countermeasures, and possibly to counterattack is vital [21]. Remote connections and organizations with geographically separated divisions or units are particularly vulnerable since they are used to dealing with Virtual Private Network (VPN) or remote access connections which can show large volumes of data flowing back and forth. Identifying a rogue connection and isolating it from valid connections can become increasingly problematic.

[1] Pharming refers to the relatively recent practice of large scale social engineering or redirecting large numbers of users to malicious web sites through techniques such as DNS poisoning.

3. Network-Centric Warfare (NCW)

In January 1998, things changed for military Information Technology. This marked the release of Vice Admiral Arthur Cebrowski and Mr. Dan Garstka's article in the U.S. Navy's "Proceedings" magazine entitled, "Network Centric Warfare – Its Origin and Future". This article, along with Alberts, Garstka, and Stein's, "Network Centric Warfare – Developing and Leveraging Information Superiority", set the stage for embracing a technological revolution in military affairs (RMA) of sorts, where the fog and friction of war would be eliminated, or at least reduced, through the implementation and adoption of technology as a warfighting capability.

The authors of "Network Centric Warfare" further define it as: "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self synchronization." [22] However, the technological hubris of the authors state that "In essence, NCW translates information superiority into combat power by linking knowledgeable entities in the battle-space."

For the authors of NCW, the concept of information superiority was born from the business world and the ability to dominate competition and a competitive advantage by applying the principles of network-centric operations. They assumed that an increase in access to relevant, accurate and timely information would have the same effect on war and warfighting as it did in the business world.

Clearly, DoD has embraced technology-centric warfighting as a way to address forced downsizing and budget constraints as well as an increase in operational effectiveness. In fact, many of DoD online portals and information technology vision statements extol the virtue of network-centric warfare and advocate technology as a critical warfighting enabler and force multiplier [23], [24]. The concern from a network security standpoint, is how integral these systems have become in day-to-day warfighting and how reliant military leaders and decision-makers have become on them for even the most routine functional services. The final analysis for strategies such as NCW is that the

DoD has passed the point of no return and that these command and control, common operational picture, situational awareness, and all-source data fusion systems must be protected as vital components of the military's arsenal. However, each system is connected and inter-connected in unique ways, often incorporating separate data feeds for weather, intelligence, logistics, medical, personnel or some other data source. These feeds and the aggregate system, or system of systems, can then be connected at various levels throughout the GIG architecture, as shown previously in Figure 3, exacerbating an already complex architecture. Additionally, this construct does not include the network security constraints imposed by business process rules, budgeting, manpower, and other forms of compartmentalization which exacerbates the network security challenges and vulnerability of the GIG.

4. The Host-Based Security System (HBSS)

The primary component of the current and future U.S. military network defense strategy is known as the Host-Based Security System (HBSS).

HBSS is a DoD enterprise-wide Information Assurance (IA) tool, based on the McAfee electronic Policy Orchestrator (ePO) product, available to support the Information Assurance and Vulnerability Management (IAVM) program and ensure secure network operations. HBSS provides centralized management of host-based capabilities and enforcing standard configurations of host machines, monitors and blocks intrusions, provides automatic signature updates, and provides capability to monitor security status from centralized console [25].

Traditionally, DoD information systems have been protected by implementing security tools such as firewalls and anti-virus software just inside the perimeter of the network. Although this protects the network from some threats and vulnerabilities, it isn't completely effective from attacks that focus on social engineering and other malicious software exploits.

HBSS provides the most common type of host-based protection in the form of desktop anti-virus software that identifies and stops known viruses. It also provides a desktop firewall solution. HBSS includes an Intrusion Detection/Prevention System at the network interface and operating system level sniffing for malicious activity. If it

detects malicious activity, the IDS terminate the offending activity and send an alert to security personnel. The IPS protects computers against malicious activity such as worms and Trojans.

Because HBSS is a DoD program, when it is finally implemented DoD-wide, HBSS is intended to provide visibility and reporting on the health of DoD the enterprise information system (i.e., the GIG.) Although HBSS is implemented at the host level, it is managed in a single, central location for each enterprise network. With policies, vulnerability patches and compliance scans flowing from the high-levels to each host within the enterprise scope of responsibility.

The DoD Host-Based Security System provides:

- Defense-in-depth
- Centralized management of host-based capabilities
- Automated Information Condition (INFOCON) support
- Host-based firewall
- Host-based Intrusion Protection
- Malicious activity damage limitation

The DoD HBSS also prevents:

- Buffer overflow attacks
- Unauthorized execution of code
    - -- Access to files
    - -- Transmission of data (data exfiltration)
- System degradation

The DoD HBSS:

- Enforces standard desktop configuration
- Mitigates “some” insider threats
- Detects rogue systems

The Department of Defense, through the Joint Task Force for Global Network Operations (JTF-GNO) and under the authority of United States Strategic Command (STRATCOM) intends to deploy the HBSS solution which includes the IPS client,

Configuration Management Agent (CMA) and *Asset 2500* (compliance software) client on over 5,000,000 servers, workstations and laptops throughout DoD.

At the heart of the DoD HBSS is the electronic Policy Orchestrator (ePO) as shown in Figure 3. The ePO is the component that stores the policies and executes the distribution and management of enforced policies at the client level.

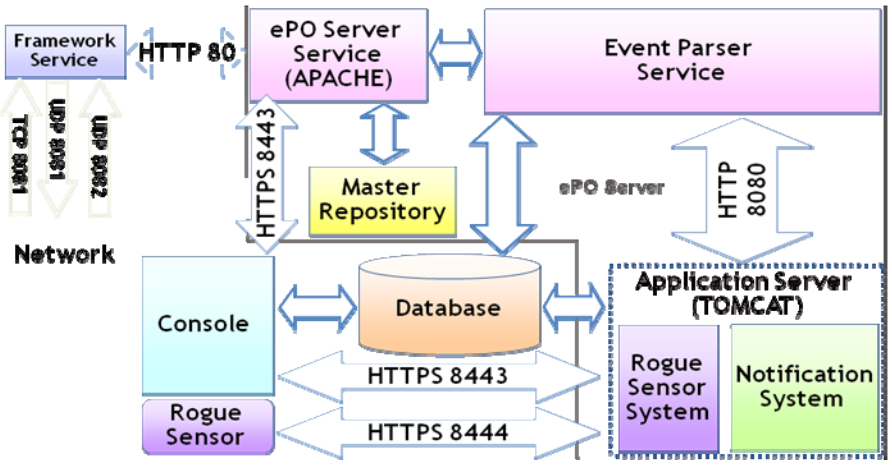


Figure 3 - DoD McAfee-based HBSS System From [25]

The ePO servers are intended to be placed strategically throughout the GIG to ensure each of the estimated 5,000,000 servers, workstations and laptops are protected and tied into the HBSS network. Each ePO is tied to the primary policy server which is controlled and updated at the DoD level by JTF-GNO.

One aspect of any enterprise defense system must be to ensure that the network is not made more vulnerable as a result of its deployment. While HBSS represents "a" solution to managing the defense of the GIG, there question remains whether HBSS will make DoD more vulnerable through the introduction of a monolithic, commercially available, single-vendor network security solution.

For example, a quick scan of known software exploits in the US-CERTs list of Common Vulnerabilities and Exposures (CVE) reveals that earlier ePO versions have been exploited several times in the recent past.

Vulnerability of the entire HBSS could result from the dynamic link library software that drives the agent on the host, or if sophisticated enough, on the ePO server itself. For example, the ePO "logDetail()" Format String Vulnerability (CVE-2008-1357) could, when exploited, cause a denial of service or allow an attacker to take complete control of an affected system [26].

Additional vulnerabilities from the U.S.-CERT National Vulnerability Database (NVD) include:

CVE-2007-1498: Multiple stack based buffer overflows allow remote attackers to execute arbitrary code [27].

CVE-2006-5271: Integer underflow allowing arbitrary code execution allows remote attackers to execute arbitrary code via crafted UDP packet causing stack corruption [28].

CVE-2006-5272: Stack based buffer overflow allowing remote attackers to execute arbitrary code [29].

CVE-2006-5273: Heap-based buffer overflow allowing remote attackers to execute arbitrary code via a crafted packet [30].

CVE-2006-5274: Integer overflow allowing remote attackers to cause a denial of service and possibly execute arbitrary code [31].

While these threats might seem few in number, the potential impact to the DoD infrastructure is enormous given the mandated reliance on this single vendor strategy by order of Communications Tasking Order (CTO) 07-012 which states:

> *The Commander, USSTRATCOM and the Commander, Joint Task Force - Global Network Operations have identified host computer defense as critical to the protection of the GIG. To protect this vital component of the GIG, HBSS is mandated for installation on all unclassified systems in the DoD, including Programs of Record. JTF-GNO CTO 07-012 [32]*

Given that the details of this implementation are not protected information, that the approved solution is commercially available software, and there are organized threats

that have the technical capability, motivation and intent to penetrate U.S. computer systems, it seems logical to assume that an adversary entity is already analyzing McAfee's HBSS ePO solution for weakness.

The limits of the U.S. domestic cyberspace include the federal, state and local government systems as well as the educational, corporate, domestic, coalition and private sectors of cyberspace. Many of these segments are interconnected to the DoD GIG through contractor, research and development (R&D), educational and even morale internet connections. Each connection increases the vulnerability of the network through the introduction of different[2] defense policies and procedures. These external connections of cyberspace are not covered by the Air Force's expenditures in network defense and will not be connected into the HBSS network.

E. A DIFFERENT APPROACH TO CYBERSPACE DEFENSE

1. Cannot "Plug the Dyke"

While many senior leaders have lived through the apparent technology driven Network Centric RMA described by Adm Cebrowski, it is clear that connectivity and interoperability have come at great cost. As our ability to communicate and interoperate has increased, so have the numbers of attack vectors and exploitable vulnerabilities within those same increasingly complex networks. Our span of control has grown to insurmountable levels while the quest for increasingly complex implementations of technology are being sought to "plug the dyke" of network threats.

While much has been said on the subject of a "Cyber 9/11" [33], or "Digital Pearl Harbor" [34] in terms of enterprise defense strategy and congressional testimony, not as much high-level attention or emphasis has been placed on the low level threats such as spear-phishing and other social-engineering based attacks. Additionally, while a "cyber 9/11" may represent a high-consequence event, the probability is extremely low. Conversely, a relatively low consequence event such as phishing attack has an extremely

[2] As systems become more interconnected, so do the firewall rule sets that exist to protect each individual network system. Without significant analysis, competing firewall rules can render enterprise networks more vulnerable, or in extreme cases inaccessible due to highly restrictive ports and protocol blocks. See Chapter III(B) for more information on this subject.

high probability of occurring. Thus, given the knowledge that phishing attacks are the most prevalent type of attack vector, and given the knowledge that phishing is not just for spam distribution but to gain access to enterprise networks, it would seem more logical that the majority of our enterprise information technology resources (e.g., funding) would be dedicated to both current and future network defense technology; including procurement and R&D.

2. Proposed Solutions

a. Intrusion Detection Systems

Fundamental to enterprise security is intrusion detection and intrusion prevention. While IDS focuses primarily on analysis of network traffic in an offline mode, intrusion prevention is designed to be an inline capability. In other words, an IDS indicates an event that has already happened, while an intrusion prevention system (IPS) indicates an event that is about to occur. Data rates, processing speeds, policy management, etc., are all contributing factors to help decide whether to employ one type of technology over another, or both.

IDSs for example, are far from perfect and may produce both false positives and non-relevant positives. Non-relevant positives are alerts that correctly identify an attack, but the attack fails to meet its objective [21]. In terms of limiting the amount of traffic detectable by an adversary who might be gathering intelligence regarding a networks defensive capability, IDSs are very noisy. In addition to false positives, they produce alerts with different levels of relevance. As a consequence, the effectiveness of alert correlation is negatively affected by the poor quality of the input alert stream [21].

Regardless of which technology is preferred by the security professional, the absence of integrated, enterprise-wide security monitoring and management may impede an enterprise's ability to respond rapidly and intelligently to cyber attacks.

This is the dilemma facing many network security strategists: Our networks are growing increasingly complex, they are connected to too many external sources, there is not enough standardization and enforcement of standards when they do

exist and laying more technology onto an already complex environment is simply making things more difficult to manage and defend.

At least one aspect of network defense can be addressed without technology; the social engineering vulnerability. Phishing, or spear-phishing, exploits the human dimension of network defense. For not even the most sophisticated firewall or IDS can prevent a user from giving their personal information away if they have been lulled into a false sense of security. Additionally, since many corporate or government enterprise users feel "safe" behind the de-militarized zone (DMZ), firewalls, IDS and other network security features of their networks, it could be argued that when a phishing email does arrive in their inbox they are even more likely to trust the source since they feel their company would not endanger their network environment by letting unauthorized email through. However, as has been seen, spear-phishing and other tailored forms of phishing attacks have been successful in breaching enterprise security, not just the average home user. Coupled with the enterprise threat, many users of government and corporate networks take their work home and through Virtual Private Network (VPN) or Secure Socket Layer (SSL) connections are able to work from home. The practice of telecommuting or remote access introduces a whole new set of "hosts" to the enterprise that are not subject to the JTF-GNO CTO mandating HBSS protection. If a home computer then, already has a backdoor (installed via a phishing, or other malicious attack) and the user accesses the corporate network via VPN, bypassing the firewall and IDS monitoring software has been made trivial for the attacker.

b. Future Technology-based Network Defense Solutions

While it is generally accepted that the term and practice of phishing (e.g., collecting personal account data from America Online users) has been around since 1996, the technology to counter the threat as well as mainstream attempts to educate users against the growing threat, has not kept pace. Some in the security industry have predicted that the technology to perform deep packet, content and contextual analysis is at least two generations away [35]. If current trends are any indication, the attackers will

have developed new methods of exploiting networks and social engineering vulnerabilities rendering future solutions obsolete before they are even fielded.

The positive aspect of this trend is that network security is moving from perimeter security to internal network security and protecting smaller groups of workers and business units versus the enterprise as a whole; as with HBSS for example. However, as previously stated, as the trend of interoperability becomes more pervasive and information sharing becomes more ubiquitous, the lines between the network boundaries becomes more blurry making network defense more challenging.

c. Network Defense as a National Strategy

For the Air Force, the first step was recognizing the warfighting domain of cyberspace [4]. The next steps included thinking about network defense from this holistic viewpoint which means building security solutions for systems in cyberspace versus systems on an enterprise network.

Understanding this distinction will be critical to moving towards a capability that both protects resources and provides a mechanism to command and control (C2) the network defense capabilities that they are tasked to protect.

The United States Government has recognized the requirement to develop this type of unified defense capability and has captured this, and other aspects of cyberspace security requirements, in the National Strategy to Secure Cyberspace (NSSC) published in 2003. In fact, the NSSC defines as its top priority, establishing a National Cyberspace Security Response System; which includes eight major actions [36].

1. Establish public-private architecture for responding to national-level cyber incidents;

2. Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments;

3. Encourage the development of private sector capability to share a synoptic view of the health of cyberspace;

4. Expand the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security;

5. Improve national incident management;

6. Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;

7. Exercise cyber security continuity plans for federal systems; and

8. Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities

The recognition of both the reliance on and vulnerability of cyberspace has raised alarms at the highest levels of the government and as a result, the president's budget has redirected billions of dollars towards research and development to meet this looming threat [37], [38].

Additionally, significant R&D requirements have been identified in the Federal Plan for Cyber Security and Information Assurance Research and Development plan [39]. This comprehensive plan takes the first steps towards developing a national R&D agenda by pulling private-sector, academia as well as governments at the local, state and federal levels together for the first time. The ultimate objective of this R&D initiative is to strengthen the security of the Nation's Information Technology infrastructure [39]. Addressing the major findings and conclusions from the report will take many years and will likely suffer the effects of funding, political priorities and other programmatic impediments but the important step of identifying the national R&D shortfalls and technology gaps has been taken.

d. Incident Response

While the majority of the actions in the NSSC's Response System requirement focus on information sharing, collaboration and coordination, improving national incident management will provide the most significant benefit to the national level and will provide a model for incident management capabilities at other levels of federal, state, local and private enterprise networks [16].

Within the United States, the organization tasked with national level incident response responsibility is a Computer Security Incident Response Team (CSIRT); a function of the United States Computer Emergency Readiness Team (U.S.-CERT), which is the operational component of the Department of Homeland Security's National Cyber Security Division [40].

The U.S.-CERT defines an incident as the act of violating an explicit or implied security policy which include but are not limited to [41].

- Attempts (either failed or successful) to gain unauthorized access to a system or its data

- Unwanted disruption or denial of service

- The unauthorized use of a system for the processing or storage of data

- Changes to system hardware, firmware, or software characteristics without the owners knowledge, instruction or consent

Figure 4 captures the complex relationship between the U.S.-CERT, tasked with domestic computer security and incident response, and over 250 different incident response and security teams around the world including various elements at the State, Local and private level. The U.S.-CERT's main coordination function is with the CERT/Coordination Center (CERT/CC)[3] of the Software Engineering Institute (SEI) at Carnegie Mellon University.

[3] The CERT/Coordination Center is the primary function of the CMU/SEI CERT® program. CERT®, as it applies to CMU/SEI, is not an acronym.

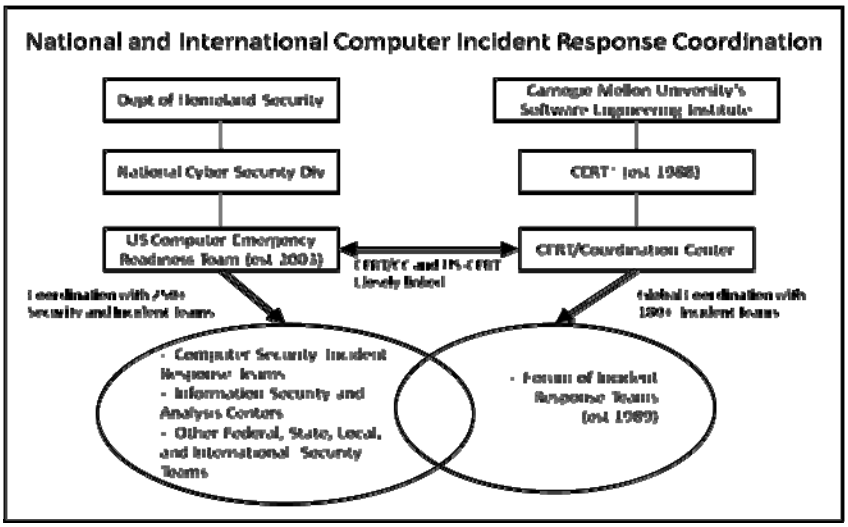


Figure 4 - Domestic and International Computer Incident Response

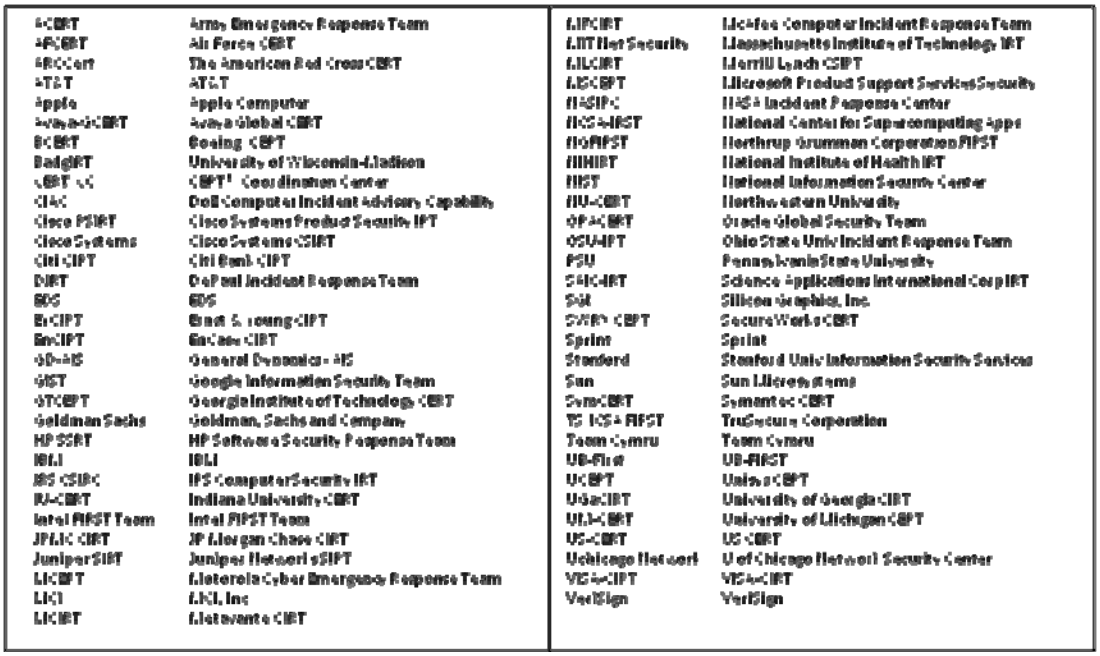
The SEI, a Federally Funded Research and Development program, was tasked by the Defense Advanced Research Projects Agency (DARPA) with establishing a computer security coordination center, the CERT® in November 1988 after the "Morris Worm" was released which demonstrated the internet's vulnerabilities to attack [42].

One year following the creation of the CERT/CC in 1988, the Forum of Incident Response and Security Teams (FIRST) was established. This organization is made up of over 180 member teams around the world and fosters coordination and cooperation to meet the growing challenges facing computer security professionals [43].

Taking an active role in enterprise security and providing the ability to respond to intrusions or other security events is a critical capability for an organization regardless of size or mission. However, this is especially true in the U.S. Government and the DoD since the Federal Government's span of control covers the 15 executive departments, 130 agencies and other organizations each with unique technical and security requirements. The ability to launch a coordinated response to a computer related incident is clearly a challenge.

Figure 5 shows the 62 U.S. organizations that are members of the FIRST organization. Note that not every agency or department in the Federal Government is

represented or covered by the FIRST organizations. The critical conclusion being that as of January 2008, there were approximately 540,000,000 hosts on the internet [44] of which only a small percentage are protected by some incident response team.



ACERT	Army Emergency Response Team
AFCERT	Air Force CERT
ARCCert	The American Red Cross CERT
AT&T	AT&T
Apple	Apple Computer
Avaya-CERT	Avaya Global CERT
BCERT	Boeing CERT
BadgIRT	University of Wisconsin-Madison
CERT CC	CERT® Coordination Center
CIAC	DoE Computer Incident Advisory Capability
Cisco PSIRT	Cisco Systems Product Security IRT
Cisco Systems	Cisco Systems CSIRT
Citi CIRT	Citi Bank CIRT
DIRT	DoPaL Incident Response Team
EDS	EDS
ErCIRT	Ernst & Young CIRT
EsCIRT	EsCase CIRT
GD-AIS	General Dynamics - AIS
GIST	Google Information Security Team
GTCERT	Georgia Institute of Technology CERT
Goldman Sachs	Goldman, Sachs and Company
HP SSRT	HP Software Security Response Team
IBM	IBM
IBS CSIRC	IBS Computer Security IRT
IU-CERT	Indiana University CERT
Intel PIRT Team	Intel PIRT Team
JPMC CIRT	JP Morgan Chase CIRT
Juniper SIRT	Juniper Networks SIRT
MCIRT	Motorola Cyber Emergency Response Team
MCI	MCI, Inc
MCIRT	Metavante CIRT
McAfee	McAfee Computer Incident Response Team
MIT Net Security	Massachusetts Institute of Technology IRT
MLICIRT	Merrill Lynch CSIRT
MSCERT	Microsoft Product Support Services Security
NASIRC	NASA Incident Response Center
NCSA-IRST	National Center for Supercomputing Appl
NGPIRST	Northrup Grumman Corporation PIRST
NIHIRT	National Institute of Health IRT
NIST	National Information Security Center
NU-CERT	Northwestern University
OPACERT	Oracle Global Security Team
OSU-IRT	Ohio State Univ Incident Response Team
PSU	Pennsylvania State University
SAICIRT	Science Applications International Corp IRT
SGI	Silicon Graphics, Inc.
SWRI CERT	SecureWorks CERT
Sprint	Sprint
Stanford	Stanford Univ Information Security Services
Sun	Sun Microsystems
SymCERT	Symantec CERT
TS ICSA FIRST	TruSecure Corporation
Team Cymru	Team Cymru
UB-First	UB-FIRST
UCERT	Unisys CERT
UGACIRT	University of Georgia CIRT
ULM-CERT	University of Michigan CERT
US-CERT	US CERT
Uchicago Network	U of Chicago Network Security Center
VISA-CIRT	VISA-CIRT
VeriSign	VeriSign

Figure 5 - National FIRST Organizations

Given the growing numbers of attacks on the internet and the increasing levels of sophistication of the adversary, and their ability to persist in numerous enterprise systems despite hardened defensive postures, the task to protect cyberspace appears to be nearly impossible.

CERTS and incident response teams must better arm themselves with the tools to rapidly deploy personnel and resources to contend with attacks. CERTs and IRTs require extensive communication to provide the critical command and control necessary to engage and remove the adversary when they are discovered on the network. This type of communication, as shown in examples provided by Dr. Ritchey and others, provides a great deal of information to anyone “listening” on the network. As his after action report showed, the attackers were monitoring the network for indications that they

had been discovered and were able to either move to other less monitored portions of the network, or disappear only to return when they knew they were not being monitored. Incidence response teams cannot afford to provide the adversary more information than they already have, however no tools exist that allow this type of interaction between team members and the many reach-back functions they must draw on to perform forensic and technical analysis.

Additionally, response teams are considered a high-demand, low-density asset. This means there are not enough of the highly trained and experienced experts in the field of network security, forensics, and incidence response that can handle the increasing numbers of threats to the many (and growing) networks. This type of trained cadre of experts cannot be developed overnight. Organizations like FIRST and the U.S.-CERT have developed the much needed coordination mechanisms necessary to share information and keep others in the field informed but there are still too few "good guys" to protect the 540 million hosts [44] from the "bad guys".

F. CONCLUSION

This chapter has focused on several complex issues that lay the foundation for a new approach to network security in an environment that is rapidly exceeding our capacity to understand with any degree of measurable certainty. As Clausewitz pointed out, warfare, at its very core, deals with uncertainty. The application of "the fog of war" is especially relevant in cyberspace where the manmade domain of electronics and technology has no boundaries and no borders. It is imperative therefore that network defense consider the boundary-less, border-less and uncertainty factors of cyberspace, and that success is predicated on addressing and overcoming not only the adversarial threats in cyberspace, but also the cyber "fog of war."

The question posed by this chapter, is whether network defense has kept up with the threat and, that in the context of historical network security trends, the most recent and most insidious social engineering threats should be analyzed as a basis for future enterprise security requirements and solutions.

Whether a solution to the cyber threat is about technology (i.e., building the better mousetrap), user education, or a combination of the two, what is clear is that the domain in which this conflict is occurring is in a constant state of change and therefore requires a new…a different…approach to network defense and ultimately to cyberspace defense.

In terms of traditional, technology-based solutions, future network defense strategies must treat cyberspace as a singular environment; the national cyberspace defense strategies, including DoD, cannot afford to segregate and isolate network defense solutions for networks that are neither segregated nor isolated. This does not mean different organizations cannot establish their own network defense polices and capabilities, however they must be created with a fundamental understanding that they are part of, and subject to the sometimes hostile environment of, cyberspace.

Since 1988, teams of highly trained network security professionals have organized to respond to direct attacks on networks as well as collaborate on current threats and mitigation strategies. However, these incidence response teams are outnumbered in terms of the networks and hosts that need to be protected as well as the increasing sophistication of the adversary that poses the threat.

As a result, new methods of organizing and responding such that the team's presence does not provide intelligence to the adversary must be developed. This technology must also allow the high-demand, low-density teams of network security professionals to respond to numerous threats throughout their areas of responsibility while collaborating to ensure other teams are aware of current threats.

THIS PAGE INTENTIONALLY LEFT BLANK

III. REAL-TIME DISTRIBUTED SYSTEMS

A. DISTRIBUTED COMPUTING

A distributed system is one in which components located at networked computers communicate and coordinate their actions only by passing messages [45]. Examples of distributed systems in every day computing environments are:

- The Internet;

- Intranets, or sub-component of the internet;

- Mobile computing environments;

Looking at the internet as a whole, it becomes obvious as to the motivation to link systems together for the purpose of sharing resources towards accomplishing goals or objectives. Tools such as file sharing, email, social networking, etc, are all accomplished using numerous resources shared by many users simultaneously. Resources throughout the system can be managed by centralized or distributed servers and accessed by clients anywhere in the system as shown in Figure 6 [45].

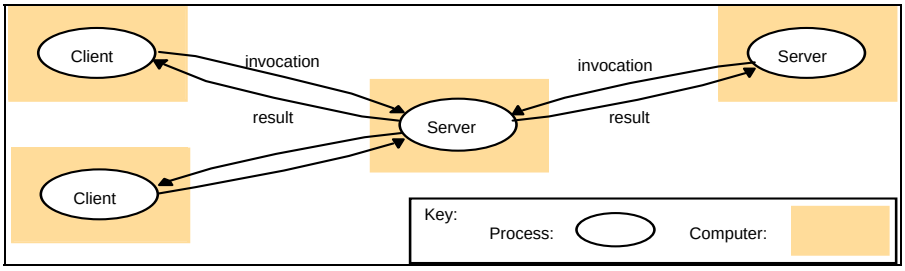


Figure 6 - Client-Server Based Distributed Systems From [45]

As components of a distributed system are linked together, numerous challenges can arise. Different operating systems, types of hardware platforms, different security

policies, scalability[4] factors, etc., are just some of the challenges facing large scale distributed system designs. When faced with geographically separate systems or hosts, issues such as concurrency[5], timing[6] and independent failure handling[7] may have significant consequences to the overall network performance characteristics.

1. Distributed Intrusion Detection

Applying the principles of distributed computing to Intrusion Detection, or network security, is not a new concept. Snapp (et al) proposed the Distributed Intrusion Detection System (DIDS) [46] leveraging much of the work from Denning [47] and Lunt [48].

The DIDS strategy was based on developing usage profiles of network resources and then comparing those profiles with historical trends to determine possible security violations [46]. Whereas much of the foundational IDS work focused on standalone (i.e., closed) networks where collecting and storing log files for large numbers of user data was a resource constraint, the proposed DIDS architecture was one of the first systems to consider the network connectivity as an attack vector and thus, required its own mitigation strategy. Later applications of the DIDS technology can be seen in intrusion detection systems that analyze user behavior patterns in real-time to determine possible malicious activity.

---

[4] While there is no universally accepted definition of scalability [99], for the purposes of this thesis the general definition is used; scalability refers to growth of computer systems to accommodate increases in users, bandwidth, or processing capability such as with routers, switches or operating system processing capability.

[5] Concurrency refers to different computers on the same distributed network performing the same function at the same time. Coordination of concurrent processing is critical to successful distributed system design [45].

[6] Timing, or a global clock is also a critical component of distributed system design and refers to the mechanism by which message passing is synchronized and disparities resolved, to a specific time standard ensuring successful processing of exchanged messages. [45]

[7] Failure handling refers to the concept that each member of the distributed system can, and likely will fail, at some point. The ability to gracefully handle such failures without affecting, or minimizing the impact of those failures on, the system as a whole is critical feature of distributed systems [45].

Distributed Intrusion Detection System technology must evolve to protect an environment that is growing faster and more complex than traditional single network defense systems can handle. Additional reasons include: [49]:

- Attacks that can only be detected by correlating data from multiple locations
- Coordinated attacks that require global scope and awareness
- Normal user and network patterns increasing false-positive indications
- Correlating data to demonstrate intent
- Automated attack patterns that overwhelm traditional IDS capability
- Numbers of attacks that overwhelm traditional IDS capability

A distributed intrusion detection strategy makes sense for a number of reasons but primarily because the Internet itself is distributed. Attacks can come from any location in cyberspace without regard to borders, international treaties, or even laws. More importantly though, distributed intrusion detection makes sense because it shifts the strategic focus away from protecting the network (i.e., network-centric), to protecting the data that traverses the network, that is, data-centric (or information-centric.)

Responding to a growing need to correlate global intrusion and network attack data across cyberspace, several systems have been developed. Three programs exist which cover the spectrum of hobby-shop distributed IDS capability, to global corporate coverage: Symantec™ DeepSight™ Threat Management System [50], myNetWatchman [51], and the Internet Storm Center (ISC) [52]. Each solution is basically a collection of feeds from numerous users throughout cyberspace (i.e., the internet), firewalls, routers, etc., that are then processed and correlated into timely, cyber events, threat warning and mitigation strategies.

As with the FIRST organization, which is an organization focused on coordinating information for cyber incident response, these “meta” IDS systems are virtual organizations without enterprise responsibility or response capability. These systems do provide a model for understanding the complexity of the cyberspace environment, however. The ISC uses the analogy of modeling and tracking global

weather patterns where large numbers of sensors placed at strategic locations are constantly monitored for temperature, wind, etc. Individually, the data from the sensors is relevant to the local area. When aggregated and analyzed by skilled network defense experts, patterns, trends and events begin to emerge that would not otherwise be detectable. This is the benefit and advantage of distributed Intrusion Detection.

2. Intrusion Tolerance

Intrusion tolerant systems represent a relatively new category of computer network defense technology recognizing that network intrusions and attacks cannot be prevented with 100% certainty. Therefore, designing systems based purely on intrusion detection (reactive defense) or intrusion prevention (proactive defense) ignores the likelihood that an adversary can, and in most cases will, breach an enterprises network defenses. As discussed in Chapter Two, social engineering techniques such as phishing or spear-phishing exploit the human aspect of computer networks which no IDS or IPS technology can mitigate. For this reason, researchers have developed this class of network defense techniques to ensure enterprise networks exhibit characteristics of survivability and reliability in the event of an attack to one portion.

System reliability is an important characteristic and design advantage of distributed technology, particularly with network defense strategies which are built upon the requirement of operational availability. Operational availability translates to system uptime, which of course is a corollary to reliability and fault tolerance.

A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked--namely, sending conflicting information to different parts of the system.

The initial research into developing a methodology to contend with these types of system faults in a distributed environment was raised by Akkoyunlu, et al [53] which was later given a name to represent the problem: The Byzantine Generals Problem[8]: [54]

[8] Imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement.

Extending the problem abstract, distributed systems are designed to deal with and tolerate arbitrary system faults which are known as byzantine faults; named for the original problem which addresses the behavior of inter-process communication and messaging. Systems that are designed to mitigate and survive these types of byzantine faults can be referred to as fault tolerant or survivable. In a distributed intrusion detection or intrusion tolerant system, tolerance refers to the ability of the system to survive an attack to a segment or portion of the network. In other words, mechanisms exist within a system to isolate the attack, or redundant mechanisms and data exist to ensure survival of the network and its resources.

Approaches to designing and implementing Intrusion Tolerance techniques differ, but the end result for any type of ITS is a network capable of withstanding and surviving a network attack. Various solutions to develop an ITS have been proposed by industry and academia such as Starfish [55], APOD [56] , ITUA [57], and Willow [58].

B. REAL-TIME COMPUTING

Real-time computing is defined as processing or computations that must occur within a specified period of time [59]. Systems are further classified as “hard” real-time or “soft” real-time, depending on the consequences of failing to meet the time constraint imposed. For example, a hard real-time system such as an automotive airbag system must operate within fractions of a second. The consequences of a misfire could be fatal, therefore system tolerances are set such that it either fires on time, or it has failed. Conversely, a cell-phone button response routine is considered a soft real-time system since the cell-phone operating system must respond before some determined delay but the tolerances are much greater and therefore the consequences are not zero.

For the purposes of intrusion detection and network security, “real-time” implies that event correlation and analysis happens as they occur, or as rapidly as otherwise possible. When coupled with distributed systems concepts, real-time requirements impose message handling constraints ensuring geographically separated, but related events are correlated, analyzed and tracked as single events as they occur. The combination of real-time processing characteristics integrated within a distributed

computing environment is an excellent solution for large-scale enterprise networks with numerous processing regions and large numbers of hosts.

Denning [47] outlined additional justification for pursuing real-time IDS capability:

1) Most existing systems have security flaws that render them susceptible to intrusions, penetrations, and other forms of abuse; finding and fixing all these deficiencies is not feasible for technical and economic reasons;

2) Existing systems with known flaws are not easily replaced by systems that are more secure-mainly because the systems have attractive features that are missing in the more-secure systems, or else they cannot be replaced for economic reasons;

3) Developing systems that are absolutely secure is extremely difficult, if not generally impossible; and

4) Even the most secure systems are vulnerable to abuses by insiders who misuse their privileges.

Network security systems today are increasingly complex and subject to numerous rules and overlapping policies [60] that can be exploited rendering networks vulnerable. Thus, the motivating factors that led to Denning's initial Intrusion Detection Expert System design [47] are even more applicable in today's network environment.

Figure 7 illustrates the correlation between firewall errors and firewall rule complexity which can lead to a decrease in overall network security. In this chart, Rule Complexity (RC) is a function of the number of rules in a firewall policy, the number of network objects affected by the rules and the number of network interface cards on the firewall itself. As the chart shows, simple firewall configuration sets are less prone to error, however in practice, less effective against external network threats. Similarly, complex firewall sets with multiple interfaces can increase the number of errors, decreasing the firewall's effectiveness.

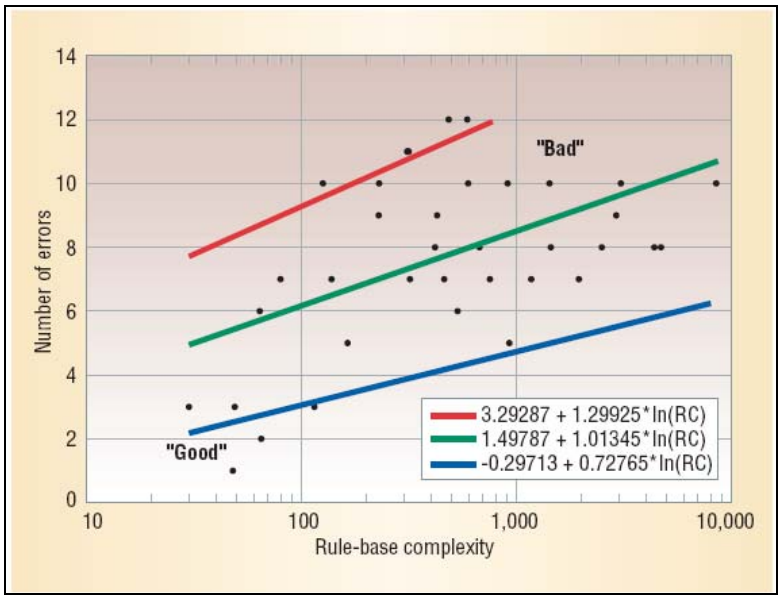


Figure 7 - Firewall Errors versus Firewall Rule Complexity From [60]

As networks grow in complexity and the connections between them increase to meet the demands of information sharing and interoperability, the response from network defense professionals is to increase the layers of defense. However, as Figure 16 indicates, there is more likely and inverse relationship between the defense-in-depth complexity and the overall security posture of the network due to the inability and complexity of managing such a system effectively.

Additionally, once these systems are integrated and operational, ostensibly to protect the network and users, in many cases the security systems cannot simply be removed without catastrophic consequences to the entire network. For example, critical Command and Control systems, or weapon control systems that are tied into mission critical network segments would have to be shut down or rebooted to accommodate security upgrades leaving vital defense systems and personnel vulnerable to attack. This is usually not an option for military leaders.

And lastly, there are no completely secure networks. Even those that are not connected to the internet or another closed system are still vulnerable to insider threat, misuse, defective code or some other form of security threat.

C. REAL-TIME DISTRIBUTED COMPUTING SYSTEMS AND STANDARDS

The delivery and receipt of information or messages is a critical component to real-time systems. In a distributed environment, message predictability, reliability, integrity become extremely challenging and a primary concern for system architects as well as network defense professionals. Factors such as bandwidth, processing capacity, network topology, security policies, operating system and hardware heterogeneity, etc., all contribute to the complexity of real-time messaging and information flow.

Middleware applies a software layer of abstraction to address and contend with these various factors. The term, middleware, defines a broad group of software and standards that assist programmers and system developers of distributed systems to ensure messages and information flow between various computers, servers, databases, etc., are able to communicate and operate effectively and efficiently. Middleware typically falls into one of three broad classes to meet these requirements:

1. Client-Server

Client-server has been the mainstay of networked systems for many years. Servers include machines that store or produce data, while clients are machines that request data. Client machines run an Application Programmer Interface (API) that allows the server to appear local to the client side. Middleware in a client-server configuration calls methods, Remote Method Invocation (RMI) on remote objects as though they were on the local machine, thus hiding the true topology of the network. Examples of client-server middleware include CORBA, DCOM and Enterprise JavaBeans (EJB) [61].

Client server architectures work well in systems with centralized data production, where many users access a central data repository—a one-to-many configuration. However, if there are multiple nodes generating data, a more complex data storing and distribution mechanism must be employed to ensure the right information gets to the servers for later redistribution of the data.

These configurations do not tend to scale efficiently as they typically utilize Transmission Control Protocol (TCP) to send information between clients and the server.

While TCP incorporates reliability in that it retries dropped packets, etc., it does not incorporate delivery semantics such as quality of service. Additionally, since TCP requires dedicated resources for each connection maintaining large numbers of these connections for large networks becomes inefficient affecting the overall scalability of the client-server environment [61].

2. Message Passing

Message passing architectures implement queues of messages as the basic design philosophy. Processes can create queues, send messages, and service messages that arrive, extending the client-server design to a more distributed architecture. At a basic level, message passing simplifies the exchange of information between many nodes on the network.

Despite the improvements over basic client-server system design, a message processing architecture does not support a data-centric[9] model of handling information due to the connection required between sender and reciever. Additionally, message passing systems rarely allow control over the messaging behaviors or QoS characteristics; messages flow and are received when produced or processed with similar expecations and delivery semantics [61].

3. Publish-Subscribe

In simplest terms, publish-subscribe middleware adds a data-centric model to messaging in the distributed environment. Publish-subscribe nodes simply "subscribe" to data they need, and "publish" information they produce with messages logically passing directly between nodes. This model implies both discovery and delivery criteria which, when coupled with message handling policies (e.g., quality of service) specifications mirrors time-critical information delivery systems such as a newspaper or magazine; hence the reference to publish-subscribe.

[9] Data-centric communications decouples senders from receivers; the less coupled the publishers and the subscribers are, the easier it becomes to extend the network in terms of scalability and flexibility [64].

However, not all subscribers in a large distributed system are interested in every event that is being published within the system. For example, network defense specialists may be monitoring for specific event alarms or thresholds which might be considered precursor events to a network attack. For this reason, various implementations of the publish-subscribe scheme have been developed; *topic-based*, *content-based*, and *type-based* [62], [63].

a. Topic-based Publish-Subscribe

One of the earliest implementations of publish-subscribe, topic-based implementations, or broker-pattern, extended the concept of communication channels used to bundle communicating peers, with specific methods that characterize and classify event content. Topics, identified and typed by keywords are similar to notion of groups, or group communication. Since the introduction of topic-based publish-subscribe broker patterns several improvements have been made such as the use of hierarchies to orchestrate topics [62].

b. Content-based Publish-Subscribe

An improvement on the topic-based patterns described above, content-based publish-subscribe patterns introduce a subscription scheme based on the actual content of the specific events versus an abstract topic, or keyword [62]. In other words, properties of the event such as internal data structure, security level or event type can make content-based broker patterns very flexible and powerful messaging construct, particularly when coupled together forming customized subscription schemes.

c. Type-based Publish-Subscribe

An extension of topic-based publish-subscribe, type-based focuses on specific data type as a way to identify the kind of data to which the user is subscribing [62]. This strategy provides a tighter coupling and integration of the language and middleware increasing system efficiency by reducing the computational overhead associated with topic-based and content-based messaging analysis.

4. Publish-Subscribe for Cyberspace Defense

Some key features that give publish-subscribe middleware an advantage in network security and cyberspace defense are:

- Publish-subscribe systems are well suited to distribute large quantities of information with minimal delay, even in the presence of unreliable or bandwidth constrained environments such as satellite links, or shared tactical links.

- Finding the correct information is trivial since subscriber nodes simply declare their interest in a topic and the system delivers it as soon as it becomes available. Similarly, sending the right data is trivial since the system publishes information as soon as it becomes available to the system.

- Publish-subscribe is efficient from a system resource standpoint since messages flow directly from source to consumer of the information without the need for intermediate servers, storage or message processing. Multiple nodes can subscribe to, and publish, the same information, introducing redundancy and fault tolerance into the system.

Publish-subscribe technology has already been incorporated into industrial design systems, stock exchanges and in some cases military weapon systems. An important step in the future evolution and success of publish-subscribe however is that it has been recognized as a capability needing approved industry standards and a formal specification and oversight group.

The Object Management Group (OMG), which maintains existing middleware standards such as Common Object Request Broker Architecture (CORBA) and Unified Markup Language (UML), has established the first international publish-subscribe standard, OMG Data Distribution Service (DDS). DDS incorporates all the features of traditional publish-subscribe middleware and increases the QoS components available to programmers and distributed system developers [61].

5. Object Management Group's Data Distribution Service for Real-Time Systems (DDS)

In the OMG DDS model, information flows using a publisher and DataWriter on the sending side of the message, and a subscriber and DataReader on the receiving side (Figure 8) [64].

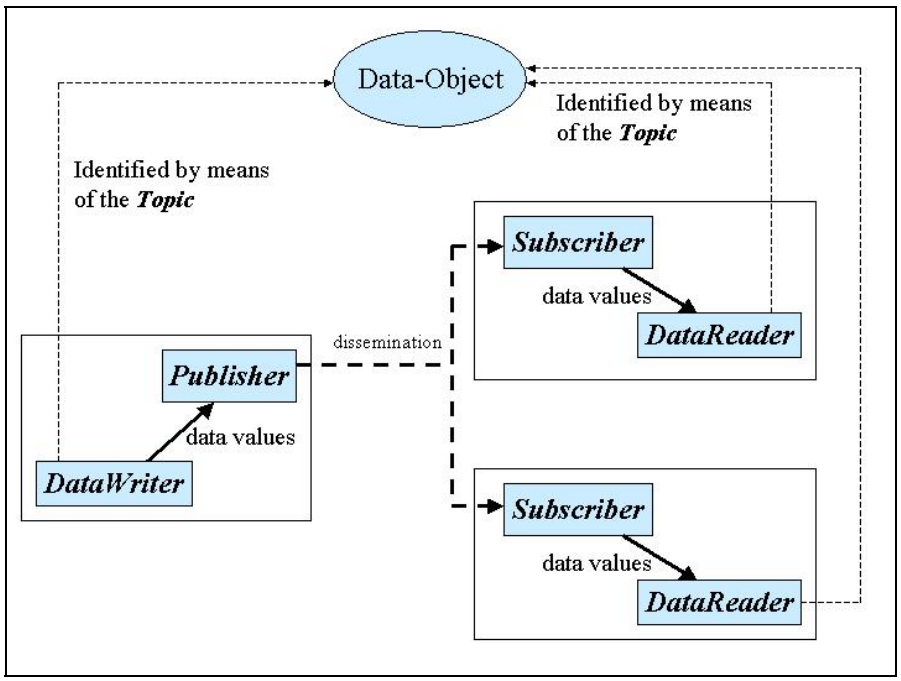


Figure 8 - OMG DDS Publish-Subscribe Model From [64]

A Publisher is an object responsible for data distribution. It may publish data of different data types. The DataWriter is the object the application must use to communicate to a publisher the existence and value of data-objects of a given type. A publication is defined by the association of a data-writer to a publisher. This association expresses the intent of the application to publish the data described by the data-writer in the context provided by the publisher [64].

A Subscriber is an object responsible for receiving published data and making it available (according to the Subscriber's QoS) to the receiving application. It may receive and dispatch data of different specified types. To access the received data, the application

must use a typed DataReader attached to the subscriber. Thus, a subscription is defined by the association of a data-reader with a subscriber [64].

Thus, DDS allows a flexible and discrete level of QoS control on either side of the communication path [64]. Additionally, DDS decouples communication at several levels adding flexibility and control to the system; in space (message nodes can be anywhere on the system – host, server, wireless), time (delivery of messages can be either immediate or at some other specified time interval), and flow (delivery can be made reliable under controlled bandwidth constraints.)

The overall distributed application, as shown in Figure 9, is composed of processes called "participants", each running in separate address space on different computers (client, server, wireless laptop for example.) Participants can simultaneously publish and subscribe to typed data-streams identified by "topics", which logically fit between specific publications and subscriptions.

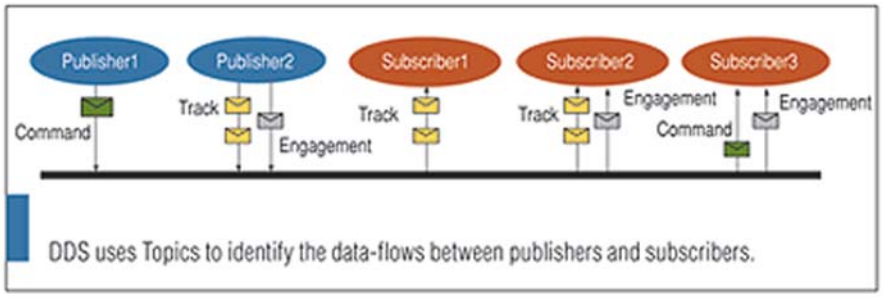


Figure 9 - Use of Topics in DDS Publisher-Subscribe Middleware From [65]

Since publications must be known unambiguously such that subscriptions can explicitly reference them, "topics" are necessary to connect publishers and subscribers. To increase scalability, topics may contain multiple independent data channels identified by "keys" allowing message nodes to subscribe to many, possibly thousands, of similar data streams with a single subscription. When the data arrives, the middleware sorts it by key and delivers it, with consideration to QoS parameters, for efficient processing.

6. DDS and Distributed Cyberspace Defense

The following section lists several important aspects of the DDS specification that illustrate its utility in a distributed cyberspace environment and which should ultimately be considered as a foundation for the next generation cyberspace defense and cyberspace C2 applications [61].

a. Complex Data Flow

Due to the implementation of QoS features, DDS is an excellent candidate for complex data flow environments. These features allow the integration of non-heterogeneous operating systems, hardware platforms and bandwidth constrained systems. These features include the ability to fine-tune different message update rates, reliability factors or bandwidth control on a per-node or per-stream basis. DDS QoS integrates various transport layers as well; from sporadic wireless connections to high-performance switched fabrics addressing factors which typically impose uneven and unreliable delivery into systems [61].

b. Latency Requirements

The DDS specification does not require a central server, therefore system implementation can leverage direct peer-to-peer, event-driven transfer. This design provides the shortest possible delivery latency. This also provides a significant advantage over traditional client-server designs as central servers and processors impose overhead and latency as an intermediate network hop that could potentially double latency time for round-trip processing. In a large-scale real-time environment, central servers receiving and correlating data from many thousands of sensors can impose severe time delays overall. Client-server designs, using and underlying TCP transport mechanism do not handle client-to-client communication efficiently due to the need for constant polling which also imposes performance constraints on the overall system. DDS QoS standards allows applications to make important trade-offs which is especially critical in bandwidth constrained environments where timely delivery and receipt of information can mean the difference between life and death. Many tactical, airborne and deployed networks fit this category where the tradeoff between reliability and low latency

is important. In heavily networked or "netted" environments where many channels are available, DDS allows applications to leverage channel prioritization, ensuring even lower latency for high priority messages [61], [66], [67].

c. Large Networks

Without the constraint of an underlying transport mechanism, or assuming the availability of reliability, DDS can take advantage of multicasting to send a single packet to any number of users that have expressed interest through subscription. Multi-casting with DDS has the added benefit of reducing message traffic, increasing overall throughput in the system [61].

d. High Data Rates

DDS implements a direct peer-to-peer connection which is determined at subscription time. When data is ready, every node already knows where to send the information, thus the actual sending process is more efficient than the typical TCP send (which requires discovery and acknowledgement) allowing DDS to publish repetitive data at very high rates. Intrusion Detection System sensor data, for example, would be very repetitive status updates which would be aggregated at various points throughout the network [61].

e. No Single Point of Failure

The DDS architecture specification does not require dedicated message handling nodes which allow the system to exist without single points of failure. This is achieved because DDS routes using a peer-to-peer connection versus through a message server. Thus, if a single node experiences a fault, the rest of the system is not affected—redundancy of publishers and subscribers is built into the system. Additionally, node failover can be configured on a per-data-stream basis giving the network transparent failover characteristics which is critical in a distributed command and control environment where dedicated backup systems must be employed to ensure survivability [61].

f. Self-healing Communication and Dynamic Configuration

DDS incorporates automatic discovery based on OMG's publish-subscribe specification. DDS allows the enterprise to be configured such that if network segments become isolated, they can continue to function with the resources available and when the network is reconnected, it will automatically rediscover the new nodes and function as an a whole entity. In terms of cyberspace defense, this feature would be most beneficial when networks are added to the GIG or other subordinate level enterprise domains to ensure there are not gaps in the network security hierarchy. The GIG is essentially a living entity, which responds to a highly dynamic global environment by constantly growing and changing. The ability of a cyberspace defense system to successfully adapt to this environment without undergoing architecture revisions, reviews, or security analysis is critical [61].

Additionally, cyberspace defenders must rethink their approach to enterprise defense and thinking of their piece of the enterprise as the extent of their responsibility. Rather, all of cyberspace must be considered in future implementations of enterprise cyberspace defense. Distributed technology, such as DDS, that allow this unbounded consideration of cyberspace will be the key to this new generation of defensive systems. Additionally, DoD cyberspace strategists must consider evolving methods of communication such as wireless and future cellular technology which effectively removes geography and location from the equation.

g. Quality of Service

The DDS specification includes over two-dozen individual QoS policies that can be applied to establish custom "contracts" between senders and receivers in the network. Some of these key QoS polices that are relevant to the design of a cyberspace defense system are:

- Data lifetime, which includes data life while the publisher is active, or data life after the publisher is no longer available to the network. This feature is critical to tactical environments where individual nodes that are publishing data might

be active for a very short timeframe but the data they publish needs to live beyond their presence on the net;

- Frequency of information updates, i.e., the rate at which updated values are sent or received;

- The maximum latency of data delivery, i.e., a bound on the acceptable interval between the time data is sent and the time it is received;

- The priority of data delivery, tied directly to the transport medium

- The reliability of data delivery and whether missed data will be retried. This policy could be tied to data priority policy to ensure higher priority data is retried, while lower priority data is not conserving network resources, particularly in a constrained environment;

- Duration of data validity; the specification of an expiration time for data to avoid delivering “stale” data which is vital in a time sensitive environment where messages must be synchronized with other entities to ensure operations are executed properly. This policy is especially important in a command and control network function.

These QoS policies are some of the features that, when coupled with type information (Figure 10), form the basis of the subscription matching mechanism of DDS and ultimately, whether publishers and subscribers can communicate [68].

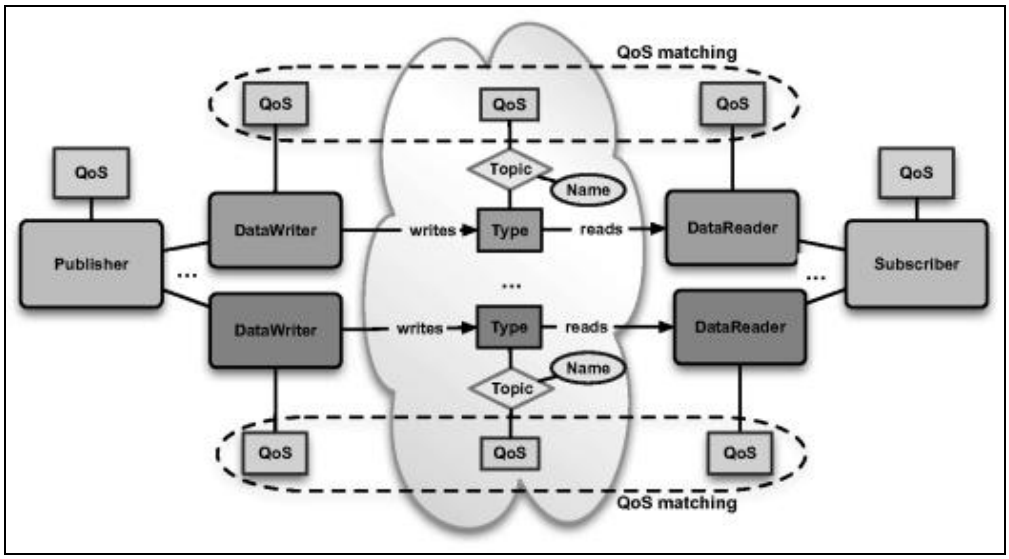


Figure 10 - DDS Subscription Matching with QoS and Type Information From [68]

This extended form of data-centric design by "contract" helps ensure systems operate as intended by its designers, both from a functional and QoS perspective.

h. Discovery

Another key design feature of DDS is that all information needed to establish communications can be discovered automatically, in a completely distributed manner. Applications dynamically declare their intent to become publishers and/or subscribers of one or more topics to the DDS middleware, which then uses this information to establish the proper communication paths between discovered entities [68].

At present, DDS is employed by two major vendors that specialize in real-time systems; Real-Time Innovations, Inc., and PrismTech, Inc. Using the OMG open specification for publish-subscribe middleware as a foundation, each company has slight differences in their implementation.

7. Real-Time Innovations DDS

The RTI implementation of DDS is based on a decentralized DDS architecture as shown in Figure 11, placing the communication and configuration-related capabilities

into the same process as the application itself. These capabilities execute in separate threads (rather than in a separate process) and are used by the middleware to handle communication and QoS [69], [70].

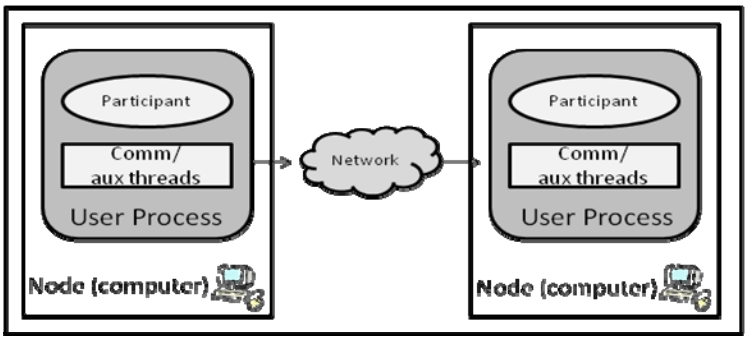


Figure 11 - RTI DDS Decentralized Architecture From [69]

The advantage of a decentralized architecture is that each application is self-contained, without the need of a separate daemon. As a result, latency and jitter are reduced because fewer context switches are involved compared to the federated architecture, and there is one less configuration and failure point.

The disadvantage, however, is that specific configuration details, such as multicast address, port number, reliability model, and parameters associated with different transports, must be defined at the application level. Requiring each application developer to handle these details is tedious, error-prone, and potentially non-portable. This architecture also makes it hard to buffer data sent between multiple DDS applications on a node, and thus does not provide the same entity-per-node scalability benefits offered by the federated architecture.

8. OpenSplice DDS from PrismTech

PrismTech Inc., uses the OpenSplice DDS which is implemented in a federated architecture, as shown in Figure 12. OpenSplice uses a separate daemon process for each network interface which must be started before all entities in the domain can communicate. Once started, each daemon communicates with others and establishes data channels based on reliability requirements (e.g., reliable or best-effort) and transport

addresses (e.g., broadcast or multicast). Each channel handles communication and QoS for all the entities requiring its particular properties. Using a daemon process decouples the entities (which run in a separate user process) from configuration and communication-related details. For example, the daemon process can use a configuration file to store common system parameters shared by communication endpoints associated with a network interface, so that changing the configuration does not affect application code or processing [69].

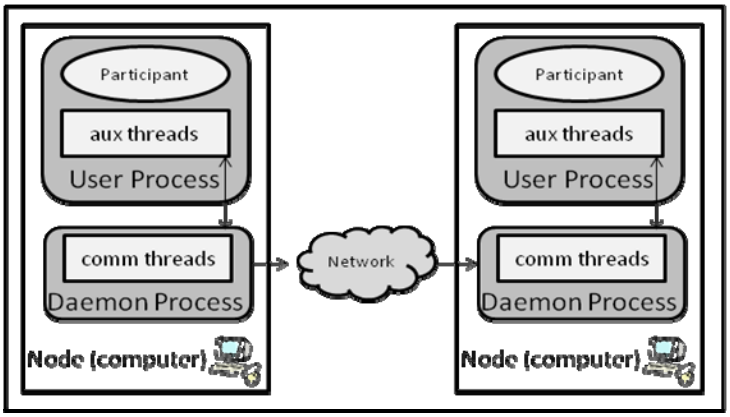


Figure 12 - OpenSplice DDS Federated Architecture From [69]

Another feature of OpenSplice DDS implementation is that it utilizes a shared-memory architecture (Figure 13) where data is physically present only once on any machine [71].

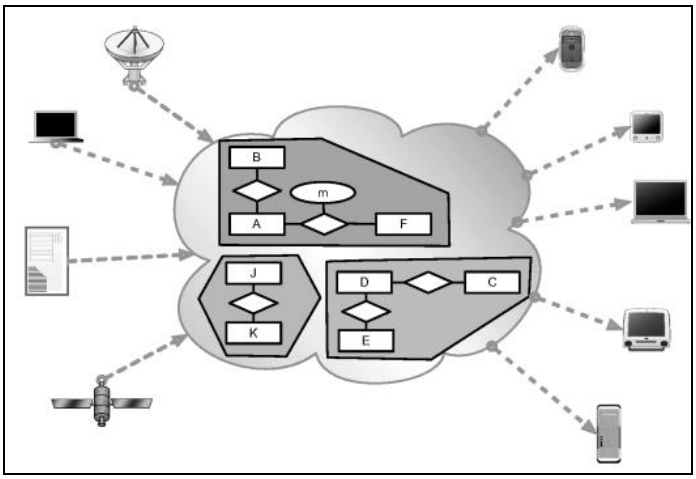


Figure 13 - OpenSplice Shared Memory Data Space From [68]

This memory architecture results in an extremely low footprint, excellent scalability and optimal performance when compared to other DDS implementations due to the fact that each reader/writer are "communication-endpoints" each with its own storage (i.e., historical data both at reader and writer) and where the data itself still has to be moved, even within the same platform, as is the case with RTI DDS.

An advantage to using a federated architecture is that in general, it allows applications to scale to a larger number of DDS entities on the same node, e.g., by bundling messages that originate from collocated entities. Additionally, using a separate daemon process to mediate access to the network can; 1) simplify application configuration of policies for a group of entities associated with the same network interface; and 2) provide a network scheduler that prioritizes messages from different communication channels.

A disadvantage of the daemon-based approach, however, is that it introduces an extra configuration step—and possibly another point of failure. Moreover, applications must cross extra process boundaries to communicate, which can introduce overhead that increases latency and jitter [69].

D. CONCLUSION

This chapter has introduced and detailed a software architecture that is well suited for a cyberspace defense system known as real-time distributed middleware using the publish-subscribe specification.

Under the context of integrated real-time software design solutions, a discussion of middleware was presented, outlining the three major categories of real-time designs: client-server, message passing and publish-subscribe.

One of the most valuable features of publish-subscribe is that it incorporates over two-dozen QoS features that are customizable at either the sender or receiver node to ensure messages are handled appropriately [69]. Each of these QoS features, coupled with the DDS automatic discovery mechanism, is a critical design criterion for an enterprise network defense or cyberspace defense system.

While the two commercial applications of DDS have their advantages and disadvantages depending on the specific system being developed, they were both developed using an open standard as the foundation. The advantage of open standards is that any software system can be developed as a Government-owned solution which has tremendous security advantages over commercially developed software that is available to any entity that can afford the product.

IV. COVERT CHANNEL COMMUNICATIONS

The use of covert channels in a distributed real-time cyberspace defense system represents a new and radical departure from traditional network defense paradigms. Our discussion of covert channels originates from the idea that information communicated between users of a networked system must be protected from adversary detection.

The obvious question raised by this idea however becomes: Why not just encrypt the communications between the users? Recall from Chapter II however that data points to the sustained presence of adversaries inside the borders of our networks. This poses a challenge even to encryption. While encryption protects the information contained within the message, it does not hide the fact that there is a message to begin with. As an example, Figure 14 shows a message exchange between two users, Alice and Bob. On a typical network this message traffic would flow between Alice and Bob through some type of network appliance (i.e., router, switch, gateway, mail server, etc.)

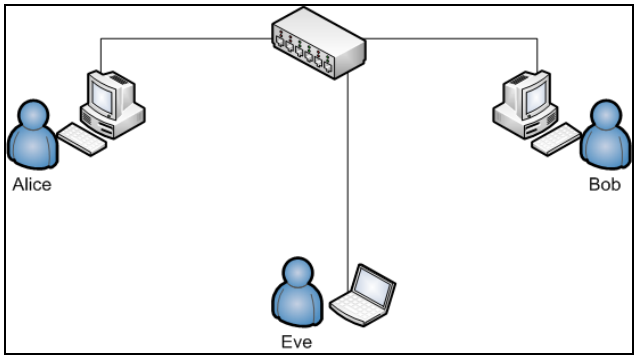


Figure 14 - Plaintext Message Exchange

Also on the same network is a persistent adversary, Eve, who is passively listening to network traffic between Alice and Bob. Since Alice and Bob are not encrypting their messages, it is trivial for Eve to intercept and extract their communication.

If Alice and Bob encrypt their messages however, as indicated in Figure 15, by the dashed lines, Eve is unable to extract the contents of the message traffic, but is still aware that Alice and Bob are communicating. Collecting message transmission characteristics (frequency, duration, recipient, etc.) over periods of time, can convey useful information to an adversary.

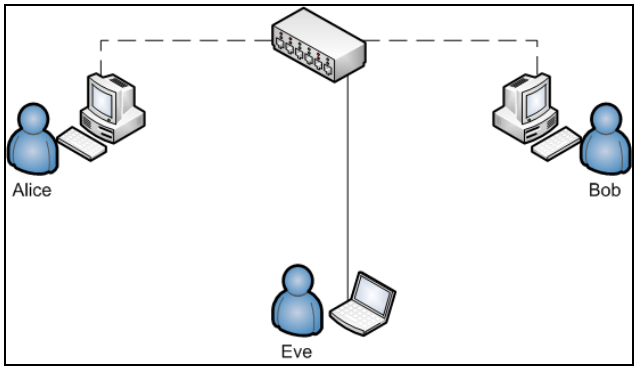


Figure 15 - Encrypted Message Exchange

For example, if Eve was trying to passively footprint or enumerate the network, she could monitor network flow across the router or switch, while watching for an increase in traffic to or from the network's security personnel. Any change in the amount of messages might be an indicator that her position had been compromised and that she should leave the network or go into hiding. Regardless, Eve did not have to know *what* was being transmitted; simply that *something* was being transmitted.

In order to prevent Eve from acquiring any information about the network, and to protect the communications between important users on the network, something other than encryption should be employed. Extending our previous example, we now introduce technology that renders the message exchange between Alice and Bob invisible. That is, from Eve's perspective, as a network traffic observer, there is no message exchange taking place, as shown in Figure 16. To Alice and Bob however, messages flow as they did in the previous two scenarios.

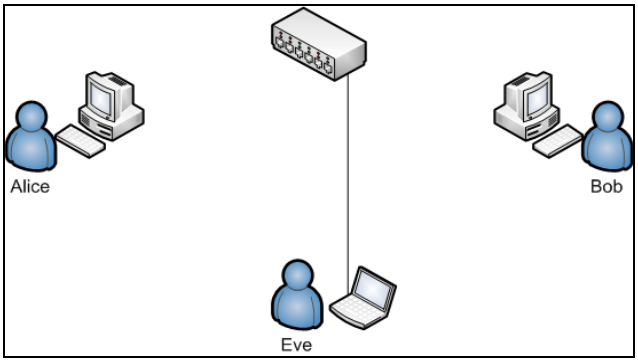


Figure 16 - Covert Message Exchange

As pointed out in earlier chapters, adversaries in cyberspace are already on the networks and are sophisticated enough to monitor critical communications between incident response teams and other critical command and control functions. In many cases, these types of communications are more valuable than mining data from the network itself because they can reveal forensic and network defense tactics, techniques and procedures which should be protected to the maximum extent possible. This is the utility and effectiveness of covert channel communications.

A. COVERT CHANNELS DEFINED

A covert channel is a mechanism that can be used to transfer information from one user of a system to another using means not intended for this purpose by system developers [72].

The term "covert channel" is typically associated with trusted computing due to the desire to prevent processes in a computer system from executing outside their intended purpose and violating some established security policy. Trust, is an important characteristic in computer design.

When a computer system is being certified for operation, particularly in a secure environment, or when the computer system is intended to process classified information, a covert channel analysis is required. This rigorous process identifies portions of the

system that could be exploited and manipulated to provide the backdoors necessary to implement a covert channel. In this context, "covert" has a negative connotation; covert is something nefarious and used for nefarious purposes and should be engineered out of the system.

However, what if the system was designed to communicate with covert channels? What if the system could be designed such that covert channels were available and used when necessary to protect the existence of information on the system and kept from being exploited by an adversary? Is there risk involved in creating covert channels for the express purpose of communicating, or does the fact that it is created make it not covert?

We begin with some basic terms and references to define what a covert channel is, and what it is not. Next, we present various methodologies of covert channel implementations and discuss how they are used.

The first use of the term "covert channels" is attributed to Lampson's "A Note on the Confinement Problem" which raised the issue of confining a program during execution so that it could not transmit information to any other program except its caller. The concern was with safeguarding data from unauthorized access or modification and that a trustworthy program must guard against any possible leakage of data [73].

From Lampson's original classification scheme, covert channel analysis has evolved into two general categories;

1) Storage channels; in which data are written to a storage location by one process and then read by another process; and

2) Timing channels; in which the timing between transmitted packets is modulated at a specific rate thereby encoding information in the sequence variations

Later analysis of communications processes [74] included both overt channels and covert channels. Overt channels use the system's protected data objects to transfer information. That is, one subject writes into a data object and another subject reads from the object. Channels, such as buffers, files and I/O devices, are overt because the entity used to hold the information is a data object; that is, it is an object that is normally

viewed as a data container [74]. Overt channels are controlled by enforcing the access control policy of the system being designed and implemented.

Extending the term covert further and by using some of the semantics of overt channel communication, it is clear that "covert" can mean more than just an adversary attack/communication vector. In fact, many covert channels are classified as benign, which carry the following characteristics [72]:

- The sender and receiver is the same subject; for example in the ex-filtration of data, an attacker would remove or copy information remotely, to themselves or to an intermediate host.

- The sender is allowed to communicate directly with the receiver under the system's security policy

- There is no effective way to utilize the signaling mechanism

In other words, covert channel communication implies that under the system's security policy, the sender and receiver are not allowed to communicate; therefore there must be a mechanism which can be exploited which allows sender and receiver to communicate despite the policy constraints of the system.

Clearly, there is confusion. Even the word, "covert" has implications beyond the original connotation of Lampson's use of the term. The American Heritage Dictionary for example, simply states for the definition of "covert": concealed; hidden; secret [5].

Oblietely, et al [75], traced the evolution of the term "covert channel" through research and scientific journals to discover that indeed, there is no clear consensus as to what the fundamental definition should be. Their analysis revealed no less than eight different definitions beginning with Lampson's original usage of the phrase, "covert channel:"

Definition 1: Covert channels are those not intended for information transfer at all, such as a service program's effect on the system load [73].

Extending the relationship of covert channel to the confinement problem first identified by Lampson, we then get;

Definition 2: A covert channel is a communication channel that is based on transmission by storage into variables that describe resource states [76].

As the confinement problem context evolved into a differentiation between storage and timing categories, a newer definition emerged;

Definition 3: Covert channels are those channels that are the result of resource allocation policies and resource management implementation [77].

In the early 1980s, the DoD published its Trusted Computer System Evaluation Criteria which defined covert channels in a fairly traditional sense as:

Definition 4: A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy [78].

A newer, refined definition followed from McHugh, which attempted to integrate intent and motive into the definition with;

Definition 5: A covert channel is any mechanism that can be used to transfer information from one user to another using means not intended for this purpose by the system developers [72].

Closely following McHugh's definition of intent, we saw the application of covert channel applied to network security environments, specifically firewalls with;

Definition 6: A covert channel is any mechanism that can be used to communicate between two parties through secured boundaries of data [79].

Another more generalized definition followed from Marone's analysis;

Definition 7: A covert channel is simply the transfer of data between two processes that are not permitted or not known to be in touch with each other [80].

The IEEE collaborated and developed a definition which they qualified as, "a necessary but not sufficient" definition;

Definition 8: A covert channel is a channel between a sender and receiver at different levels and there is a Trojan horse present that uses a communication medium other than a named object [81].

In an attempt to clear up the confusion, the authors of [75] chose to establish their own definition based on two factors; 1) that a definition of covert channel should encompass both storage and timing channels, and 2) there should be an association between the use of a channel and the violation of a security policy;

Definition 9: A covert channel is an unintentional communication path which results from a system's resource allocation and management implementation and violates the system's security policy [75].

Millen [82] and Morone [80] refined the definition to exclude the characteristics of information hiding, which occurs when the two communicating parties are allowed to talk; for example the use of steganography implies hiding information as opposed to covert channels even though the function of the steganographic medium is the same. Millen's definition of covert channels states:

Definition 10: Covert channels are a means of communicating between two processes that are not permitted to communicate, but do so anyway, a few bits at a time, by affecting shared resources [82].

In Millen's terminology, a channel's distinction as covert is directly related to the security policy of the overall system: If the policy allows the communication, but the communication is not observed, then the information is simply *hidden*. However, if the security policy does not allow the communication, and the communication still takes place, then the channel employed is *covert*.

Because there is no universally accepted definition of covert channel communication, further discussion of what is, or is not; covert yields little in terms of substantive academic progress. Rather, we stipulate that *covert* recognizes the concept of protecting communication from observation, whether the information is hidden overtly,

or whether the communication channel is covertly violating the design of the security mechanisms built into the system [75], the end result should be the same: protected communication.

Specific characteristics of covert channels such as bandwidth[10], channel capacity[11] and noise[12] factors associated with various channel implementations are beyond the scope of this thesis and should be considered in the system requirements and design phase. For this reason, we continue the discussion of protecting communication by exploring specific network-based and distributed system covert channel implementations for the purpose of designing an efficient and effective communications mechanism that can be integrated into a cyberspace defense capability.

B. NETWORK BASED COVERT CHANNEL IMPLEMENTATIONS

The network based covert channels discussed below focus primarily on exploiting the data fields of network protocols that are used to communicate information, synchronization, etc. Many of these standard fields are redundant or rarely used creating opportunities for numerous covert channel implementations. However, the application of most network covert channel implementations remains limited due to the fact that while they take advantage of network protocols, they communicate information in a point-to-point or one-to-one situation. In other words, they do not scale beyond single user implementations and are thus inadequate in a distributed environment with a requirement for many thousands or even millions of hosts are communicating simultaneously.

Additionally, many network protocols are not allowed through firewalls rendering network covert channel techniques ineffective in a wide area network, or cyberspace environment [83]. Protocol headers can be inspected for modifications or statistically

[10] Covert channel bandwidth is defined by [75] as, "the rate in bits per time unit at which information is communicated."

[11] Covert channel capacity is defined by [75] as "its maximum possible error-free information rate in bits per time unit."

[12] Noise in a covert channel refers to the presence or absence of errors. A noiseless covert channel is one in which the probability that the receiver receives exactly the message the sender sends is 1. [75]

significant data such as source or destination address that are outside the range of normal, indicating the presence of a covert channel.

One aspect of covert channel communication that is especially important in a wide-area network system design is anonymity; where the communication between sender and receiver must be "unlinkable." In other words, communication between sender and receiver might be observed, but the observer cannot determine who is communicating with whom [83].

Extending this concept of *unlinkable*, communication is also said to be *unobservable* if the observer cannot determine if messages are being sent at all. Thus, unlinkable and unobservable anonymity are the most desirable traits of a network covert channel designs which can also be applied in a distributed system.

The following network-based covert channel techniques represent some of the more promising examples of this type of technology which should be considered for future research and integration into an objective full-spectrum cyberspace defense capability.

1. Addressing Channel

This type of channel, first reported in 1987, uses the destination address field in the IP header as a mechanism to transmit information. The sender and receiver must first agree on a block of addresses which will be used in the channel construct, for example a block of 16 addresses. The sender then sends any type of IP message to one of the 16 addresses. The receiver, in this case, a wiretap, or network observer, picks up the presence of a message to one of the 16 addresses, each of which represents a specific code. After receiving network traffic based on a predetermined synchronization start time and duration, the receiver can then decode a message based on which addresses received a message and when.

2. Data Block Length Channel

Using the data block length, a sender can transmit a message by changing the length of the message for each IP packet. A message of length 65, for example, would

correspond to the ASCII tables and indicate the letter “A”. The sender simply sends messages with specific lengths which correspond to the predetermined code to the receiver who reads the length of each packet discerning the intended message. One of the assumptions with this method is that the sender and receiver are allowed to exchange messages.

3. IP Fragmentation Channel

This method uses the Do Not Fragment (DF) bit in the IP packet to transmit information between sender and receiver. The DF bit is used to prevent fragmentation of messages larger than the network’s Maximum Transmission Unit (MTU.) If however, the sender and receiver intentionally send messages smaller than the MTU, the DF is ignored by the system and can be utilized as a binary communication mechanism; set to either a one or a zero. This method can suffer data loss if the MTU is unknown which can be the case if the packets are traversing multiple networks and routers. As with the Data Block Length channel, it is assumed the sender and receiver are allowed to communicate directly.

4. Steganography in Networking using Toral Automorphism

The combination of steganography applied to overt channel communications represents a possible solution to the dilemma of networking with covert channels. While networks pose a particularly challenging aspect to covert channels due to the widespread employment of intrusion detection, firewalls, scanners, sniffers, traffic analysis, etc., steganography coupled with overt channel techniques have the greatest potential to keep communications unobserved.

Ashan and Kundur [84] [85] proposed a solution to this problem by exploiting concepts from digital image watermarking known as toral automorphism systems. Toral automorphism describes mathematical transformations using lattices to deform an image and produce a new image unrelated to the original. This highly complex algorithm scrambles the original producing a high level of randomization. These features of the toral automorphism systems make them useful in covert channel communications to ensure unlinkability and unobservability [83].

In the first technique, Ashan suggests using toral automorphism to develop a look-up table, mapping each letter of the alphabet to an 8-bit binary value. The selection of the 8-bit mapping is highly random and occupies the first half of the IP ID field. The second 8-bits of the IP ID field are independent and randomly generated having no relation to the first 8-bit message portion [83], [84].

In the second technique, Ashan extends his use of toral automorphism to packet sorting. His method takes advantage of the mathematical idea first raised by Shannon, [86], that given a set of *n* objects, a maximum of $\log_2(n!)$ bits can be represented. Thus, for n=25, 83.7 bits can be communicated. Using toral automorphism, the sender applies the resorting algorithm a specific number of times on the normal packet sequence to be transmitted. This re-sequenced set of packets is then transmitted to the receiver, who reorders them based on previous knowledge of the keys used to order the packets in the first place [84].

5. Protocol Hopping Covert Channel

Data hiding techniques in networks typically incorporate HTTPS, tunneling, IPSec or VPNs to protect sensitive information. However, as previously discussed, the mere presence of these tunnels or VPNs indicates, to some degree, a certain level of information that can be valuable to an adversary. Thus, one solution to utilizing traditional tunneling techniques is to employ more than one protocol to transmit a single message or information flow. The Protocol Hopping Covert Channel Tool (PHCCT) [87] is an open source proof-of-concept solution that allows the user to define what types of protocols to use, and in what order they should be employed. They can also be used using a randomized code to, as with a frequency hopping system [87].

C. COVERT CHANNELS IN DISTRIBUTED SYSTEMS

1. ACK Channel

This method applies in networked systems with built-in security that restricts message transmission between users of different security levels. For example, a sender with a higher classification cannot send messages to a receiver of lower classification.

Rather, information must flow from low classification to high. In this environment, exploiting the TCP protocols acknowledgement, ACK, message can be used to transmit information. In this case, the sender has control of acknowledging messages from the receiver and can delay the ACK response based on predetermined time duration. This delay indicates either a zero or a one bit. The receiver measures this time delay and interprets the message accordingly.

2. DBMS Channel

In many distributed network environments, the only shared resources are database files that multiple users must interact with simultaneously. Extending this to a multi-level or secured environment, transactions are regarded as higher or lower depending on the nature of the client process initiating them. In this case, the DBMS tracks whether users can read, write or both depending on the set security policy.

For example, assume that the sender and receiver are allowed to read but only the receiver is allowed to write to a specific file. The sender initiates a transaction which establishes a read lock on the file. The receiver, accessing the same file then has to wait until the lock is released by the lock manager of the DBMS (as in 2-phase locking.)

This mechanism can be employed on individual data items within a database to increase the number of "bits" with which to transmit information. In other words, the sender reads or does not read data items that the receiver also has access to. Each read lock transmits a "1" and the absence of a read lock transmits a "0" [88].

D. CONCLUSION

Covert channel communications represent an opportunity to protect valuable information. While this contradicts traditional definitions of covert channels, as outlined in Chapter II, the need to integrate some degree of covertness is critical and should be embraced by cyberspace system designers.

This chapter introduced several techniques and technologies that should be investigated further for their potential integration into a cyberspace defense system providing realistic network defense capabilities using distributed system architecture.

In a networked environment, covert methods typically exploit the transport protocols which allow messages to flow between systems or even between networks. Addressing, data block length, IP fragmentation, etc., are all relatively simple examples that lay the foundation for further study. More advanced techniques involve multiple technologies that, when integrated, establish even greater covertness, including steganography to create a covert channel riding on an overt communication medium as with Ashan's toral automorphism technique. Another open source tool under development is the protocol hopping covert channel software which is similar to frequency hopping techniques in traditional radio communications.

Distributed communications represents a more complex environment to develop covert channels, however two potential methods could be incorporated; the ACK channel and the DBMS channel. Both techniques take advantage of the shared resources that exist in a distributed network environment and also integrate a higher level of anonymity than with network covert channels, which is highly desirable in any covert system design.

1. Further Reading on Covert Channels

Additional covert channel techniques are discussed in [75], [83], [89], [90], and [91]. Methods of detecting covert channels and analysis of covert channel characteristics such as bandwidth and detectability are available in [75], [83], [92], [93], and [94].

THIS PAGE INTENTIONALLY LEFT BLANK

V. CASE STUDY – CYBER OPERATIONS INFORMATION SYSTEMS

In order to propose a solution to the requirement of creating an effective cyberspace defense capability an evaluation of network defense, real-time distributed and covert channel technology and strategies was performed. While much research has been accomplished in each area, there has been no work, to date, where all three have been brought together as a single integrated solution.

One solution was identified that brought two areas together; network defense and real-time distributed systems technology. This chapter evaluates the main features of this system and proposes a strategy to integrate the third feature, covert channel communications.

A. COIS BACKGROUND

Recognizing the need for an improved network defense capability, U.S. Space Command, the National Security Agency, and the Defense Advanced Research Project Agency/Defense Information Systems Agency Joint Program Office sponsored an Advanced Concept Technology Demonstration project called Active Network Intrusion Defense (ANID) in 2001. The goal of ANID was to demonstrate a capability to respond in real time to network intrusions by making changes to network devices like routers, firewalls, intrusion sensors, etc. The ANID system incorporated features such as a highly distributed architecture with intrusion detection capabilities installed at very low levels, and a collection of smart agents to correlate sensor information and distribute summary level alert information to neighboring nodes.

Following the successful demonstration of ANID, the Missile Defense Agency (MDA) evolved the technology into a full-spectrum cyber warfare command and control (C2) and battle management (BM) system called the Cyber Operations and Information-warfare System (COIS.) The first application of the COIS technology was deployed with the National Aeronautics and Space Administration (NASA) through a joint research endeavor between several government organizations.

The COIS application is a cyber defense system that provides cyber warfare situational awareness while supporting collaboration among members of the various operational communities known as Information Assurance (IA) Operation Centers (IAOC). The IAOC construct was initially conceived and developed through a collaborative effort between the Missile Defense Agency and the Institute for Defense Analysis and ultimately became the cornerstone of the COIS capability [95]. The IAOC also enables COIS to provide a virtual collaborative environment among members within an organization or functional community, among members of similar organizations or functional communities, or even among members of dissimilar or geographically dispersed organizations or communities [96].

COIS enables the collaboration of experts in various fields, at different NASA locations, with different sets of roles and responsibilities, through the creation and operation of *virtual communities*. COIS provides cyber warfare situational awareness, including a real-time common operating picture of the status of NASA networks and any ongoing attacks or cyber operations. It also provides a unification of all personnel performing IA; the IAOC. This team has access to a broad base of information sources within COIS which allows them to collaborate, use tools, conduct research, and act in concert across organizational and role related lines [96].

Frequent users of COIS access the system by clicking an icon on their main window and logging in. Experts in various cyber warfare disciplines, invited to participate in cyber operations during exercises or in other special situations, gain controlled access to specific relevant information presented by a limited part of the system through a secure channel.

1. Purpose of the System

COIS prototyping began after a thorough analysis of the current state of network defense systems proved that current technology was inadequate and would become increasingly inadequate as networks and information technology became more complex, more interconnected and that fewer technical personnel would be involved in the management and leadership of network defense and cyberspace operations. NASA

identified four key areas that highlighted the cyberspace defense problem that led to the original COIS requirement: strategy, awareness, knowledge and organizational problems.

a. Cyber Defense Strategy Problems

- Current network defense strategy is unrealistically narrow and primarily focuses on keeping attackers out of the network. New strategies must consider how to remove threats once they are discovered and how to mitigate the damage to an enterprise that is global in scope

- Current strategy fails to recognize the fundamental concepts of cyber warfare. Recognizing that cyberspace is in fact, a warfighting domain has recently taken hold within the Air Force however this recognition is new and must be developed rapidly to effectively counter the growing threat. NASA suggests several new approaches: maneuver (keeping assets in motion to avoid detection or from being destroyed), hunt-and-kill techniques employing mobile agents to autonomously "guard" borders and patrol internal networks, and developing more effective methods to attack and destroy hidden enemy assets (e.g., rootkit hunters.)

b. Cyber Defense Awareness Problems

- We don't know when intruders enter our networks
- We don't know our current network configurations
    -- Scans are not managed and done routinely
    -- We do not know all of our network device configurations
    -- We don't know if the configurations we do know are correct and effective
- We do not know the integrity of our enterprise systems
- We do not know the integrity of our data
- We do not know our cyberspace situational awareness

-- What is our Cyber Order of Battle?

-- What is our current attack situation (red and blue)?

-- What courses of action are available at any given time for a specific attack scenario?

-- What are the standing rules-of-engagement should an attack occur?

c. Cyber Defense Knowledge Problems

- We do not know how to design secure, real-time networks

- We do not know the software architecture of our current systems well enough to design effective network defense capabilities to protect them. For example, are we using peer process architectures, client-server, middleware, etc.?

- We do not know if our system designs are correct. Have they been designed to some standard? If so, has configuration management been utilized to ensure modifications and upgrades also adhere to standards? Can we demonstrate that our designs are correct?

- We do not truly know the extent of our current network defense appliance installations. How many are in place, at what boundaries, at what organizations, how are they interconnected and managed? What is their placement strategy to ensure proper placement and management?

- Our network security staff is inadequately trained to deal with the aforementioned issues as well as future threats to the enterprise.

d. Cyber Defense Organizational Problems

- Traditional hierarchical C4ISR organizational structure is inappropriate for cyberspace defense and cyberspace operations

-- DoD must recognize that traditional methods for organizing for cannot adapt to the speed, number and dynamics of cyber attacks

-- Traditional hierarchical organizational constructs do not permit commanders to be in multiple locations simultaneously (e.g., responding to a Distributed denial of service (DDoS) attack)

-- Traditional, organizational constructs that lend themselves to business process decision making do not promote rapid, time sensitive decision making and decision dissemination

B. COIS OVERVIEW

The developers of COIS recognized the need to link traditional network offense and defense technology with recent developments in computer technology in order to respond to the requirements defined by their initial capability gap analysis. Traditional solutions such as IDS, perimeter sensors, firewalls and encryption were not meeting the expectation and complex demands of their analysis. Non-traditional techniques such as virtual organizations, mobile agent technology, publish-subscribe middleware and collaborative messaging was necessary to close the requirements gap. However, no single technology could provide the complete solution, so facets from each were integrated into a single full-spectrum cyber warfare command and control (C2) and battle management (BM) system.

1. Virtual Cell Organizational Model

COIS employs a unique structure to place cyber operators in the midst of their domain allowing them to combat threats regardless of the location. Figure 17 illustrates this organizational cell construct and captures the differences between virtual cells and physical cells which would be tasked to support cyber operations across an enterprise. The virtual construct has several key advantages to a physical response organizational construct; mobility, rapid response, stealth and overcoming constraints of a high-demand low-density asset [96].

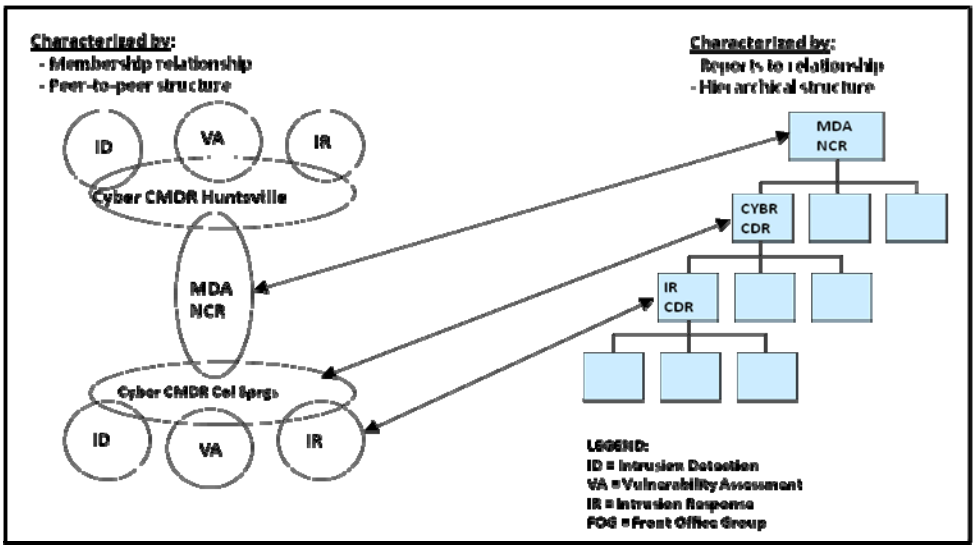


Figure 17 - COIS Virtual Cells versus Physical Cells From [96]

As the figure indicates, virtual cells are more flexible than physical cyber defense cells in that they can stand-up when needed or re-locate when and where needed regardless of logistical constraints such as travel time, personnel availability or other resource issues. They also provide a more operationally relevant construct to manage, respond to, and mitigate adversary threats on the network. Cells responsible for specific cyber operations such as Intrusion Detection (ID), Vulnerability Analysis (VA) or Incident Response (IR) can organize in a peer-to-peer fashion versus the traditional hierarchical that often constrains physical network defense organizations. This ability to peer enhances collaboration and information sharing by providing direct message exchange between cells without the impediments of a vertically organized management system. As the figure also indicates, the virtual cell can fall back into a traditional hierarchical organization when not in response mode, or for administrative reasons, preserving unity-of-command and centralized control, decentralized execution principles [96].

Additionally, virtual cells can be in multiple locations simultaneously; a powerful force multiplier considering the high-demand, low-density cyber operations personnel that are at the center of each cell organization. As organizations within the DoD and across the Federal Government face increasing budget constraints, virtual cell constructs

provide a logical means to extend the reach of existing personnel across the enterprise saving the enormous costs of education, training and career management.

One of the most powerful benefits of virtual cells is that they allow near real-time response to events regardless of the location in the organization or across the enterprise. In terms of time-sensitive responses, whether offensive or defensive, virtual organizations make the most sense within the domain of cyberspace where borders and boundaries are nonexistent and unaffected by the tyranny of distance.

a. Virtual Cell Members

COIS organizes the Information Assurance Operations Center (IOAC) virtual cell by breaking membership into one of three categories: Core Members, Associate Members, and Consulting Members [96].

- Core members, as the name implies, are full-time members of a specific community within the IOAC (ID, IR or VA for example) and perform the day-to-day tasks supporting cyber defense within the enterprise [96].

- Associate members participate and share information but to not execute or make decisions that impact the network [96].

- Consulting members are specialists brought into a community for a specific event or response action. They have limited access to the COIS data and are not involved in the decision making process [96].

b. Core Communities

NASA has identified seven core communities that ultimately comprise the IOAC virtual organization: CIO, Cyber Warfare (CW), ID, IR, VA, Network Operations (NETOPS) and the Testbed communities. Each community has full-time members that may or may not be collocated to meet the needs of their respective geographic or functional area of responsibility. Associate and consulting members may join communities as necessary when seeking information or specific technical expertise [96].

- **Chief Information Officer (CIO)**: Is responsible for direction of cyber warfare activities across the enterprise including assessments, vulnerability analysis, recovery operations, etc., [96].

- **Cyber Warfare (CW)**: These communities are assigned to regional HQ locations and coordinate with the CIO community for direction. CW communities assess regional vulnerabilities, attacks and responses and perform day-to-day and long-rang cyber planning in support of CIO requirements [96].

- **Intrusion Detection (ID)**: These communities detect activities such as adversary reconnaissance, attacks or intrusions in support of their CW community. They are also responsible for network forensics of compromised systems in support of other community entities. The ID community is responsible for day-to-day and long-range planning of how and what to monitor under their span of control [96].

- **Intrusion Response (IR)**: The IR community develops appropriate (pursuant to legal and proportional rules of engagement established by the CW community) responses to computer and network attacks. They maintain a library of responses and design (in conjunction with the Testbed community) new response capabilities. They are also responsible for damage assessment to adversaries as a consequence of attack through COIS [96].

- **Vulnerability Assessment (VA)**: The VA community is responsible for discovering potential vulnerabilities in networks under their span of control and reporting them to the CW community who determines mitigation strategies. The VA community reviews policies, operating procedures as well as information flow in and throughout their assigned portion of the network for trigger events such as modem connections, password policy enforcement, software patch status, network scans, etc. The VA community monitors other VA inputs such as CERTS and JTF-GNO as well as open-source organizations to maintain current status of network vulnerabilities [96].

- **Network Operations (NETOPS)**: The NETOPS community ensures availability of computer and network resources to accomplish the mission of their respective area of responsibility. They take input from the ID and VA communities and

ensure identified weaknesses and vulnerabilities are fixed or mitigated. The NETOPS community maintains DNS servers, e-mail servers, and perimeter assets such as firewalls, switches and routers. They also ensure workstations within their span of control are configured, patched and maintained to standards [96].

- **Testbed**: The Testbed community facilitates communication and collaboration among internal and contractor engineers and other organizations working with the IAOC. In normal day-to-day operations mode, the Testbed performs operational testing and evaluation (OT&E) as well as research, development, test and evaluation (RDT&E) of current and future COIS technology integration. During crisis actions, the Testbed resources can be used for contingency of operation (backup) and honeynet shunting to preserve and protect critical operational network resources [96].

- **Dynamic Communities**: Under the COIS architecture, communities can come together to form new, transient organizations (Figure 18) in support of specific, short duration requirements [96].

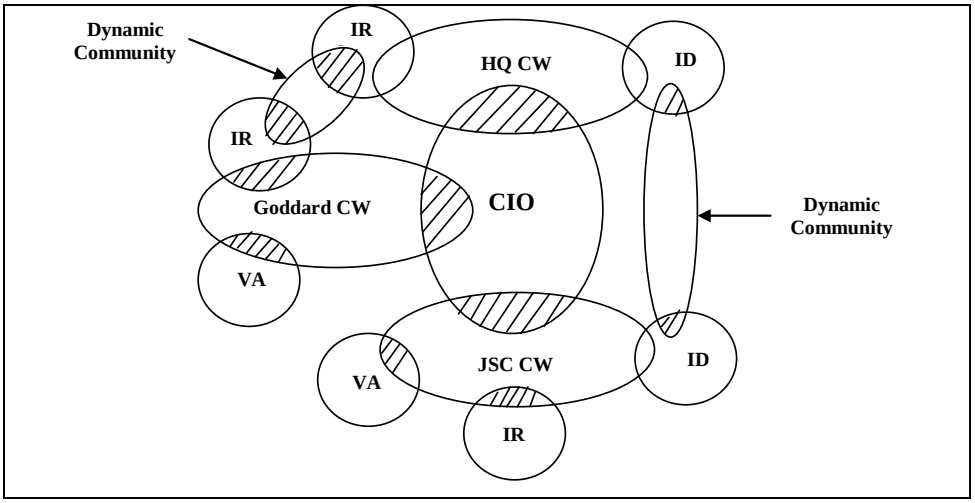


Figure 18 - COIS Dynamic Communities From [96]

Following task closure or end of operations, the dynamic community is then decommissioned. Under a virtual construct this process takes mere seconds as

opposed to reconstitution and other logistical concerns with a traditional network defense response or tiger-team. Dynamic communities can be established by any of the community directors at or below their level (e.g., a CW director cannot establish a CIO-level community, but can create a dynamic community with representatives from IA, ID or VA.)

2. Architecture

The COIS architecture takes advantage of several new technologies that allow the virtual organizational construct to exist and operate in a highly dynamic cyberspace environment. The COIS application itself is based on publish-subscribe middleware written using the OpenSplice Data Distribution Service (DDS) specification.

According to NASA, OpenSplice middleware provides the simplest architecture to implement a real-time distributed architecture and peer-to-peer collaborative messaging capability.

The COIS architecture is two-level design (Figure 19) where command and control functionality is provided through the various displays and workflow management written into the COIS software [96].

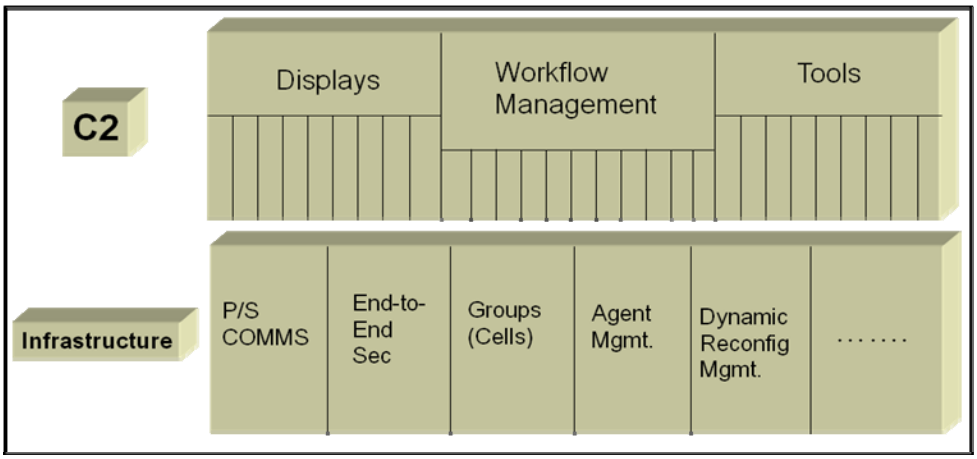


Figure 19 - COIS Architecture From [96]

Second, the COIS infrastructure provides the underlying mechanism that implements the various features of the COIS system. This infrastructure model is based on the publish-subscribe middleware but includes end-to-end security features, software agents and dynamic reconfiguration management to deliver a full-spectrum, flexible, and responsive C2 and BM cyber capability.

Mobile agent technology provides another tool in the COIS arsenal allowing the virtual organization to respond to events regardless of their location. The mobile agents are used for intrusion detection, intrusion response, vulnerability assessment and even collecting intelligence on adversary tactics for later exploitation. Since they are not static, mobile IDS agent technology is difficult for an adversary to thwart and can be quickly and easily deployed to reinforce vulnerable locations in the enterprise. This new concept of operation mimics traditional maneuver warfare tactics techniques and procedures drawing on other foundational Information Operations strategies such as military deception, psychological operations and operations security [97].

To illustrate the unified picture of COIS using various technologies; Figure 20 shows the linkages possible between various units in the NASA organization.

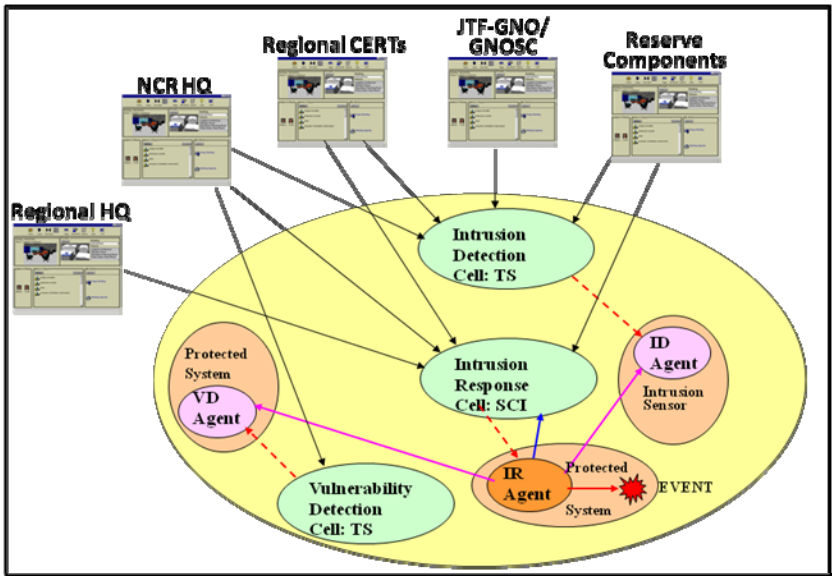


Figure 20 - COIS Strategic Operational Model with Mobile Agents From [96]

Direct lines of communication (shown as the link between HQs, CERTS and JTF-GNO), virtual cells (shown as the ID, IR and VA cells), mobile agents (reflected by processes spawned from their respective cells and running inside traditional protected network defense assets) and publish-subscribe messaging technology (which provides the critical communication and rapid C2 dissemination capability) are all combined to provide a full-spectrum cyberspace operational construct; C2, Battle Management, Situational Awareness, Communication [96].

C. INTEGRATION OF COVERT CHANNELS

As several of the figures illustrate, communication is an integral component in the COIS architecture. Communication or electronic messaging is the tie between communities in the virtual organizations and is the key to their successful execution of CIO guidance throughout the continuum of cyber conflict. Messaging flowing from publish-subscribe architecture also drives much of the mobile agent activities as well as the real-time collection and aggregation of time sensitive situational awareness information on the network. Messaging becomes and even more critical aspect of the COIS architecture than with traditional physical cyber defense organizations due to the dependence on the virtual organization construct.

For example, consider an organization with three geographically separated HQ elements, A, B, and C, each of which has an organic cyber defense capability consisting of an Intrusion Detection section, an Incident Response section and a Vulnerability Analysis section. Each HQ element is responsible for the operations and management of their own provisioned portion of the overall enterprise. An adversary is able to penetrate the HQ C network by exploiting a host through spear-phishing and implants a Trojan sniffing program to collect intelligence on as much as possible about the entire organization. We will evaluate this scenario against two notional organizational constructs; a traditional physical hierarchy, and a virtual-based hierarchy (Figure 21.)

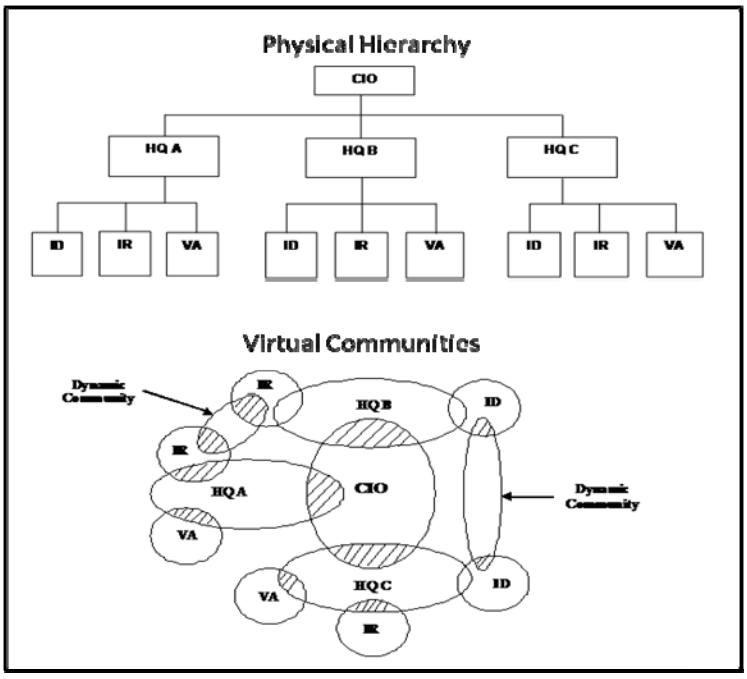


Figure 21 - Traditional versus Virtual Vulnerabilities After [96]

If our example organization employed a traditional cyber defense hierarchy, the adversary would be limited to the information they could collect. In other words, it would be unlikely they could collect information on HQ A or HQ B as they are geographically separated and isolated on a different portion of the enterprise. Rather, the adversary's sniffer, passively collecting intelligence data, is only able to read traffic that is traversing the HQ C portion of the enterprise.

If, on the other hand, the example organization employed a virtual cyber defense hierarchy which was interlinked with ID, IR or VA communities from other HQ elements, the potential to collect information on those other elements is much greater as the virtual organization provides a means to gain access to portions of the network simply by listening in on the traffic from the dynamic community that was created between various HQ elements. They strength of the virtual organization thus, can become the vulnerability of the entire architecture.

We therefore, propose a method by which messages exchanged between virtual organizations are transmitted through publish-subscribe middleware using a covert

channel protocol enabling communication without compromising the actions and intent of the cyber operators and ultimately, the organization.

In Sections IV(B) and IV(C), several covert channel techniques were discussed that are potential candidates for inclusion into a system such as COIS. The obvious advantage to developing this capability with systems like COIS, as opposed to other types of commercially available solutions, is that COIS utilizes open standard publish-subscribe middleware. The OMG published specification for DDS provides the framework to integrate unique messaging protocols to fit specific needs and requirements such as protected communication between virtual organizations. While the implementation of covert channel communications in a real-time distributed system is not trivial, given the tools provided by the OMG specification, the task is not impossible. One impediment to such an approach is that with the exception of COIS, data-centric real-time distributed systems for cyber operations have not been looked at with any wide-spread acceptance in the information technology business sector. The majority of the network defense solutions available today fall within the network-centric client-server based architecture, but as Chapter II pointed out, traditional client-server network defense systems fall short of protecting, detecting and reacting to the complex environment of cyberspace.

Another advantage is that while COIS was developed using off-the-shelf software, the program is government owned (i.e., the source code and executable files are under government control) which provides added protection of the code-base by limiting its availability to potential adversaries. In contrast, the example cited in Chapter II, McAfee's electronic Policy Orchestrator (ePO), was not developed to an open standard, but is commercially available, greatly increasing the availability to adversaries who wish to study the software for the nefarious purpose of developing exploits, which has already taken place in previous versions of the ePO software.

VI. CONCLUSION

For it is an unfortunate fact that, while peace is our goal, we need greater military security to prevent war.

John F. Kennedy [98]

A. SUMMARY

The war in cyberspace has already begun. It takes place every day, all across the globe and is fought with speed and anonymity that kinetic warfighters are struggling to understand and defend. War in cyberspace defines a new threat, one in which a single computer can be the asymmetric launch point for a massive invasion against the United States or our allies. Therefore, it is incumbent upon the United States to defend against current adversaries, and prepare for even greater threats.

An important aspect of preparation is understanding the nature of the environment in which war will be waged. In other words, what is the nature of cyberspace? Where does it begin? Where does it end? Who owns it? If no one entity owns it, how is it divided such that its pieces can be adequately defended? What does "ownership" in cyberspace really mean? How do the laws of war and proportionality apply to cyberspace and cyber operations? How does attribution and international law restrict or allow military actions in cyberspace?

While these and many other questions regarding conflict in cyberspace are beyond the scope of this thesis, we must begin to address the larger problem by scoping the issue to our own provisioned portion of cyberspace; the DoD's portion known as the Global Information Grid.

Cyberspace, or network defense, transcends the roles between military and civilian. The military is not a business, however, and our reasons for defending computer systems and networks are not the same as for many businesses and corporate network defense strategies. Despite this fundamental difference, many technology strategists looked to the business industry as a model for developing network infrastructures,

enterprise governance models and even DoD network defense capabilities. This was the so-called revolutionary strategic concept of network-centric warfare.

Chapter II illustrated the dilemma this strategy has created for today's cyberspace operations. Network-centric concepts proliferated and have increased the complexity and configuration management of today's digital battlespace. Unfortunately, they have also made it increasingly difficult to realistically defend. For the military, the task of defending our provisioned portion of cyberspace falls to the JTF-GNO, as sub-component of STRATCOM, which has the global mission to protect and defend the DoD Global Information Grid. Their latest strategy to protect and defend cyberspace relies on the Host Based Security System (HBSS); a commercial product that distributes servers throughout the infrastructure which communicate to hosts throughout the DoD. The suite of tools includes patching, desktop configuration and a personal firewall to protect individual computer systems. The HBSS relies on a single-vendor strategy, which has already been compromised and exploited in the commercial sector. It also relies on a hierarchical organizational structure to communicate information and control resources throughout the system. Additionally, there is no C2 function or incident response capability embedded in HBSS.

While client-server architectures, such as HBSS, are well suited for traditional enterprise computing environments, they do not scale or adapt to tactical and other bandwidth constrained environments, which must also be protected and defended. Additionally, military networks are constantly changing as tactical, operational and strategic threats change. The ability to rapidly adapt to the dynamic environment of cyberspace is a critical requirement to defending cyberspace whether it is a mobile wireless tactical network feeding time critical data to a battlefield command post, or adding a large bandwidth weather feed to a base infrastructure in the U.S. Each must be protected and defended as the cyberspace topology changes.

Real-time distributed systems represent technology well suited to provide this type of capability. It is designed to process and share information between geographically dispersed entities through a well organized and structured message sharing process (e.g., the internet.) As the term also implies, *real-time* information is

processed as it is produced and/or received within the system. While there are different types of distributed system messaging schemes, arguably, the publish-subscribe method has the most relevance in terms of building a cyberspace defense capability.

Chapter III details the architecture of publish-subscribe and discusses two of the major implementations that are currently available and are built upon an open standard; Real-Time Innovations Distributed Data Service (DDS) and PrismTech OpenSplice DDS. Current military real-time distributed applications focus on rapid message sharing and information processing; sometimes on the order of millions of messages per second to meet the demands of weapon system or telecommunications system design requirements. If a cyberspace adversary has infiltrated a system, these messages represent a major vulnerability both in terms of data that can be exfiltrated as well as intelligence that could be used to gain further insight into system design and operational capability.

Real-time distributed systems incorporating the publish-subscribe architecture are an excellent starting point for an enterprise cyberspace defense capability. However, military requirements for sensitive processing demand increased capability; protected publish-subscribe messaging. In this context, protected communication goes beyond encrypted or secure methods of message exchange.

Systems have been developed to encrypt information, which merely scrambles the data being transmitted such that the intended recipient can only decrypt it. However, the fact that data is being transmitted at all can still reveal a great deal of information. For example, an adversary who has compromised a system can passively watch network packet traffic flowing through the system. If network traffic increases between system administrators and say, a network intrusion or forensics team, that might be a good indication that they have been alerted to the adversaries presence and they should move on to other networks or simply lay low until it is safe to resume their activities. The cases presented in Chapter II clearly indicate that this is not a hypothetical situation. Cyberspace adversaries are developing methods to gather intelligence while on our systems, and have the ability to detect when our responses threaten their activities. In order to counter this level of sophistication, the publish-subscribe protocol employed by an enterprise, distributed system must employ covert-channel communications to

effectively hide the existence of specific types of message traffic. By doing so, this protects the overall system and allows incident response and cyber C2 actions to occur without detection.

The characteristics of covert channel communications imply that information is transmitted without detection either by using non-standard methods (e.g., storage channels or timing channels), or by using steganography to hide information in an overt communication channel. Various techniques, discussed in Chapter IV could be leveraged and applied as a new broker-pattern protocol for the publish-subscribe middleware introduced in Chapter III.

Finally, we presented a case study of the Cyber Operations and Information System (COIS) developed to provide a full-spectrum C2 and Battle Management cyberspace capability. COIS is built upon the OMG DDS specification using OpenSplice as a framework for its publish-subscribe messaging capability. The main feature of COIS is in the use of virtual organizations to meet the demands of cyberspace defense in a geographically dispersed enterprise. By leveraging the capabilities of real-time distributed technology, NASA organizations can respond to an incident anywhere in their enterprise, tapping resources from specialists at any other location. This unique approach ensures the high-demand low-density network defense specialists can be in multiple locations simultaneously.

B. STRATEGIC RECOMMENDATIONS FOR NEXT GENERATION CYBERSPACE DEFENSE

This thesis outlined key components of existing technology and network defense strategies that, when combined, form the basis for a next generation full-spectrum cyberspace defense capability. Traditional network defense, real-time distributed systems and covert channel communications are the triad of foundational technologies that form this construct. Figure 22 summarizes material presented in Chapters II, III, and IV highlighting specific characteristics that provide technological contributions to the unified cyberspace defense capability.

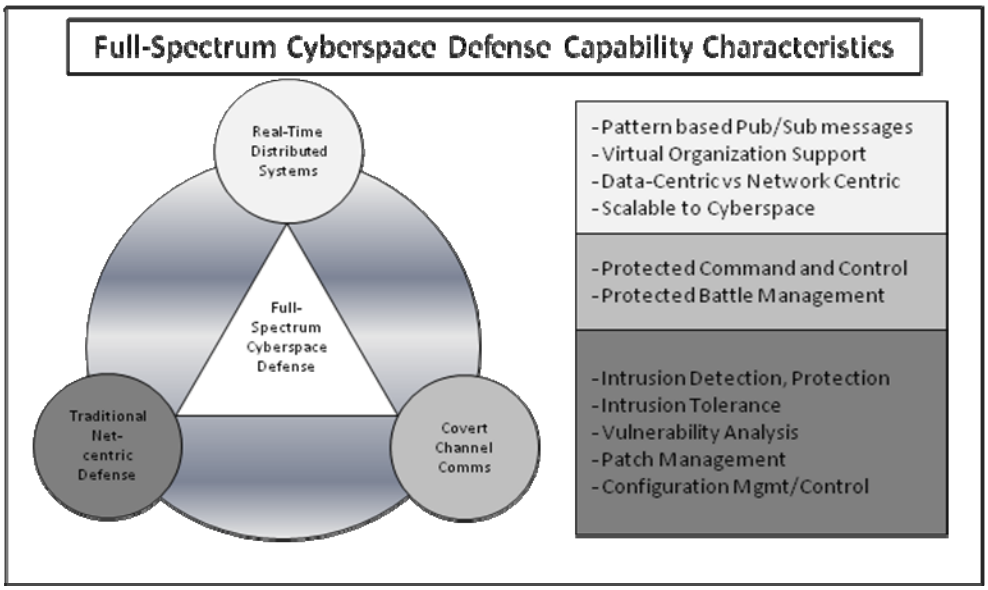


Figure 22 - Full-Spectrum Cyberspace Defense Characteristics

1. Traditional Network Defense Capabilities

Leverage features of HBSS including Intrusion Detection, Intrusion Prevention, Vulnerability Analysis and Patch Management, Desktop Configuration Management.

Include Intrusion Tolerance Systems as a GIG strategy. A fundamental shift in how DoD approaches cyberspace defense must first recognize that intrusions are going to happen. The truly relevant question is how should the DoD (and to a larger degree the U.S. Government) respond to attacks, isolate them, minimize the collateral damage caused by the attack and then recover from the attack as rapidly as possible? A network defense strategy that focuses only on keeping the adversary of the network amounts to a digital Maginot line, which is as ineffective at keeping network intrusions from occurring as it was for keeping Germany out of France during World War II.

2. Real-Time Distributed Systems

Leverage features of the COIS cyber defense capability including its use of real-time distributed system and publish-subscribe middleware, virtual organizational construct, and mobile agent technology as an offensive and defensive weapon. Mobile agent technology should also be evaluated for use in configuration management and system baselining applications.

Distributed systems technology needs to enable a unified command and control process to ensure global scope and coverage while implementing and executing a centralized operational control structure.

Migrate away from network-centric defense strategies towards data-centric or information-centric defense strategies. This approach will allow cyberspace defense to focus on protecting the information traversing the network rather than protecting the network itself.

3. Covert Channel Broker Pattern Technology

Add covert channel communication technology to protect specific aspects of the cyber defense messaging. Not every message in a cyber defense system needs the protection afforded by a covert handling mechanism. Likely candidates for covert handling include C2 and Battle Management capabilities.

C. AREAS OF FUTURE RESEARCH

1. Cyberspace and Network Defense

- Research is needed into how to measure and mitigate social engineering attacks, which will continue to be an attack vector of choice for cyberspace adversaries. Attack mitigation should not focus solely on technology however, but should also leverage user education as a primary means to thwart these types of intrusions.

- Development of new acquisition strategies that focus on data-centric solutions rather than network-centric solutions.

- Purchasing network defense solutions is a challenging endeavor. Data-centric systems will cross numerous enterprise networks and will require considerable coordination and management to integrate and operate. The DoD is currently not organized to acquire systems in this manner. Rather, DoD funds, acquires and maintains systems for individual networks and enterprises. The HBSS solution mandated by JTF-GNO for example, is a single solution for DoD but is being purchased and operated by individual service components, extending the flawed network-centric model. New funding methods must be developed that address this deficiency.

2. Real-Time Distributed Systems

- Investigation into scaling distributed systems to include tens of millions of hosts across the federal government to address data-centric versus network-centric design limitations

- Publish-Subscribe broker pattern designs to facilitate integration and implementation across multi-level secure distributed systems.

3. Covert Channels and Information Protection

- Developing a suite of covert channel publish-subscribe protocols for implementation in an enterprise cyber defense capability

- Developing adaptive techniques to avoid active detection by an adversary

- Leverage work on protocol hopping as a covert communication mechanism [87]

- Develop port hopping (a range of ports used to transmit messages) as an additional technique, possibly using port and protocol hopping simultaneously to decrease detectability (multiple protocols over multiple ports increases the randomization and covertness of the message transmission.)

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] B. Sterling, "Speech to the National Academy of Sciences," May 1993.

[2] CNN. (1999, Feb), “Internet Time: Will the ‘beat’ go on?”, CNN Science and Technology. [Online], http://www.cnn.com/TECH/computing/9902/26/t_t/internet.time/, accessed June 2008.

[3] C. V. Clausewitz, *On War,* 1st ed.. London, England: Kegan Paul, Trench, Trubner and Co., 1908, Translated by J.J. Graham.

[4] Air Force Cyber Command (P), "Air Force Cyber Command Strategic Vision," 2007.

[5] Houghton Mifflin Company, *The American Heritage Dictionary of the English Language*, W. Morris, Ed. Boston, MA: Houghton Mifflin Company, 1976.

[6] W. H. Ware, "Security Controls for Computer Systems," R-609-1, 1970.

[7] R. Gedda. (2005, Jul.) InfoWorld. [Online]. http://www.infoworld.com/article/05/07/22/HNhackermetnick_1.html, accessed April 2008.

[8] Anti-Phishing Working Group. (2008, Jun.) Anti-Phishing Resources. [Online]. http://www.antiphishing.org/word_phish.html, accessed June 2008.

[9] Oxford Information Services, Ltd. (2008, Mar.) MillerSmiles.co.uk. [Online]. http://www.millersmiles.co.uk., accessed April 2008.

[10] US CERT. (2008, Jun.) US CERT Security Publications. [Online]. http://www.us-cert.gov/reading_room/#news, accessed April 2008.

[11] R. Kessler. (2008, Mar.) Newsmax.com. [Online]. http://www.newsmax.com/kessler/internet_botnet_threat_/2008/03/24/82567.html, accessed March 2008.

[12] C. W. Williamson. (2008, May) Armed Forces Journal. [Online]. http://www.armedforcesjournal.com/2008/05/3375884, accessed May 2008.

[13] SANS Institute. (2007, Nov.) SANS Institute. [Online]. http://www.sans.org/top20/, accessed April 2008.

[14] B. T. Contos, *Enemy at the Water Cooler*. O'Reilly Media, Inc., 2006.

[15] R. Ritchey, "Forensics Case Study: How Nation States are Attacking the US Industrial Base," 2007.

[16] Department of Homeland Security, "The National Strategy to Secure Cyberspace," 2003.

[17] T. Greene. (2008 , Apr.) Network World. [Online]. http://www.networkworld.com/news/2008/040908-rsa-hack-power-grid.html, accessed April 2008.

[18] Office of the Secretary of Defense, "Annual Report to Congress - Military Power of the People's Republic of China," 2008.

[19] Senate Armed Services Committee, "Hearing of the Senate Armed Services Committee - Annual Threat Assessment," Testimony of Director National Intelligence, Mr. Michael McConnell, 2008.

[20] Department of Defense Chief Information Officer, "Global Information Grid Architectural Vision ," Department of Defense, 2007.

[21] R. A. Kemmerer and G. Vigna, "Hi-DRA: Intrusion Detection for Internet Security," in *Proceedings of the IEEE*, vol. 93, No. 10, 2005.

[22] D. S. Alberts, J. J. Garstka, and F. P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP, 1999.

[23] DoD NII. (2008, Jun.) DoD CIO, ASD (NII). [Online]. http://www.defenselink.mil/cio-nii/, accessed June 2008.

[24] DoD Force Transformation. (2008, Jun.) DoD Force Transformation. [Online]. http://www.oft.osd.mil/, accessed June 2008.

[25] McAfee Inc, *HBSS 101 Admin Course*. 2008, Document downloaded from DISA Information Assurance Support Environment secure website. Accessed April 2008.

[26] L. Auriemma. (2008, Mar.) French Security Incident Response Team. [Online]. http://www.frsirt.com/english/advisories/2008/0866, accessed March 2008.

[27] US-CERT/NIST.(2007, Mar.)US-CERT National Vulnerability Database. [Online]. http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-1498, accessed April 2008.

[28] US-CERT/NIST. (2007, Jul.) US-CERT National Vulnerability Database. [Online]. http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-5271, accessed April 2008.

[29] US-CERT/NIST. (2007, Jul.) US-CERT National Vulnerability Database. [Online]. http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-5272, accessed April 2008.

[30] US-CERT/NIST. (2007, Jul.) US-CERT National Vulnerability Database. [Online]. http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-5273, accessed April 2008.

[31] US-CERT/NIST. (2007, Jul.) US-CERT National Vulnerability Database. [Online]. http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-5274, accessed April 2008.

[32] Joint Task Force-Global Network Operations (JTF-GNO), "CTO 07-012," 2007.

[33] R. Singel. (2008, Jan.) Wired. [Online]. http://blog.wired.com/27bstroke6/2008/01/feds-must-exami.html, accessed April 2008.

[34] J. Schwartz. (2007, Jun.) International Herald Tribune. [Online]. http://www.iht.com/articles/2007/06/24/business/cyber.php, accessed April 2008.

[35] K. J. Higgins. (2007, Nov.) Dark Reading. [Online]. http://www.darkreading.com/document.asp?doc_id=140121&f_src=darkreading, accessed March 2008.

[36] US-CERT. (2005, Jun.) US-CERT. [Online]. http://www.us-cert.gov/press_room/050215cybersec.html, accessed April 2008.

[37] Foreign Policy. (2008, Apr.) Foreign Policy. [Online]. http://www.foreignpolicy.com/story/cms.php?story_id=4241, accessed April 2008.

[38] Subcommittee on Networking and Information Technology Research and Development, "Supplement to the President's Budget for FY2009 - The Networking and Information Technology Research and Development Program," 2008.

[39] The Interagency Working Group on Cyber Security and Information Assurance, "Federal Plan for Cyber Security and Information Assurance Research and Development," 2006.

[40] US Computer Emergency Readiness Team. US-CERT. [Online]. http://www.uscert.gov/aboutus.html, accessed April 2008.

[41] US-CERT. US-CERT. [Online]. http://www.uscert.gov/, accessed May 2008.

[42] CERT/Coordination Center. (2008, Jan.) CERT. [Online]. http://www.cert.org/meet_cert/meetcertcc.html, accessed April 2008.

[43] Forum of Incident Response and Security Teams. (2008) FIRST.org. [Online]. http://www.first.org/, accessed March 2008.

[44] Internet Systems Consortium. (2008, Jan.) Internet Systems Consortium. [Online]. http://www.isc.org/index.pl?/ops/ds/host-count-history.php, accessed May 2008.

[45] G. Coulouris, J. Dollimore, and T. Kindberg, *Distributed Systems Concepts and Design, 4th Ed*. Pearson Education Limited, 2005.

[46] S. R. Snapp, et al., "A System for Distributed Intrusion Detection," 1991.

[47] D. Denning, "An Intrusion Detection Model," 1987.

[48] T. F. Lunt, et al., "IDES: A Progress Report," 1990.

[49] R. Robbins, "Distributed Intrusion Detection Systems: An Introduction and Review," 2002.

[50] Symantec Corporation. (2008) Symantec. [Online]. https://tms.symantec.com/Default.aspx, accessed April 2008.

[51] L. Baldwin. (2008) myNetWatchman.com.

[52] SANS Institute. (2008) SANS.org. [Online]. http://isc.sans.org/, accessed April 2008.

[53] E. A. Akkoyunlu, K. Ekanadham, and R. V. Huber, "Some constraints and tradeoffs in the design of network communications," in *Proceedings of the fifth ACM symposium on Operating systems principles*, 1975, pp. 67-74.

[54] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," SRI International, 1982.

[55] K. P. Kihlstrom and P. Narasimhan, "The Starfish System: Providing Intrusion Detection and Intrusion Tolerance for Middleware Systems," in *Proceedings of The Eighth IEEE International Workshop on Object-Oriented Real-Time*, 2003.

[56] M. Atighetchi, et al., "Adaptive Cyberdefense for Survival and Intrusion Tolerance," 2004.

[57] T. Courtney, J. Lyons, H. V. Ramasamy, W. H. Sanders, and M. Seri, "Providing Intrusion Tolerance with ITUA," in *Supplemental Volume of the 2002 International Conference on Dependable Systems & Networks (DSN-2002)*, Washington D.C., 2002.

[58] A. Wolf, et al., "Bend, Don't Break: Using Reconfiguration to Achieve Survivability," in *Proceedings of the Third Information Survivability Workshop (ISW2000)*, Boston, MA, 2000, pp. 187-190.

[59] National Instruments Corporation. (2006) National Instruments. [Online]. ftp://ftp.ni.com/pub/devzone/pdf/tut_3938.pdf, accessed April 2008.

[60] A. Wool, "A Quantitative Study of Firewall Rules," 2004.

[61] S. Schneider and B. Farabaugh, "Is DDS for You?," 2006.

[62] P. T. H. Eugsters, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, "The Many Faces of Publish/Subscribe," 2003.

[63] A. Corsaro, L. Querzoni, S. Scipioni, S. Tucci-Piergiovanni, and A. Virgillito, "Quality of Service in Publish/Subscribe Middleware," 2006.

[64] Object Management Group, *Data Distribution Service for Real-Time Systems v1.2*. Object Management Group, 2007.

[65] G. Pardo-Castellote. (2005, Apr.) Cots Journal Online. [Online]. http://www.cotsjournalonline.com/home/article.php?id=100296&pg=1, accessed April 2008.

[66] R. Bharadwaj, "What is SINS?," in *Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC'05)*, vol. Volume 2, 2005, pp. 11-12.

[67] R. Bharadwaj, "Secure Middleware for Situation-Aware Naval C2 and Combat Systems," in *Proceedings of the The Ninth IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS'03)*, Washington D.C., 2003, p. 233.

[68] D. C. Schmidt, A. Corsaro, and H. Van't Hag, "Addressing the Challenges of Tactical Information Managment in Net-Centric Systems With DDS," no. 03, 2008.

[69] M. Xiong, J. Parsons, J. Edmondson, H. Nguyen, and D. C. Schmidt, "Evaluating Technologies for Tactical Information in Net-Centric Systems," 2007.

[70] Real Time Innovations. (2008) RTI. [Online]. http://www.rti.com/products/data_distribution/RTIDDS.html, accessed March 2008.

[71] PrismTech, Inc. (2008) PrismTech.

[72] J. McHugh, *Covert Channel Analysis: A Chapter of the Handbook for the Computer Security Certification of Trusted Systems*. Portland, OR: Naval Research Laboratory, 1995.

[73] B. A. Lampson, "A Note on the Confinement Problem," 1973.

[74] R. A. Kemmerer, "A Practical Approach to Identifying Storage and Timing Channels: Twenty Years Later," in *Proceedings of the 18th Annual Computer Security Applications Conference*, 2002.

[75] W. Oblitely, J. L. Wolfe, and S. Ezekiel, "Covert Channels: The State of the Practice," 2005.

[76] M. Schaefer, B. Gold, R. Linde, and J. Scheid, "Program Confinement in KVM/370," in *Proceedings of the ACM National Conference*, 1977, pp. 404-410.

[77] J. C. Huskamp, "Covert Communication Channels in Timesharing Systems," 1978.

[78] Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD*. Department of Defense, 1985.

[79] A. B. Ruighaver and A. Ahmad, "How Safe is Your Firewall: On the Security of Intranets," in *Proceedings of the 7th Australasian Conference on Information Systems*, Hobart, Australia, 1996, pp. 601-608.

[80] M. Marone, "Adaption and Performance of Covert Channels in Dynamic Source Routing," 2003.

[81] IEEE, "Minutes of the First Workshop on Covert Channel Analysis," 1989.

[82] J. Millen, "20 Years of Covert Channel Modeling and Analysis," in *Proceedings of the 1999 IEEE Symposium on Security and Privacy* , 1999.

[83] R. Sbrusch, "Network Covert Channels: Subversive Secrecy," 2006.

[84] K. Ahsan and D. Kundur, "Practical Data Hiding in TCP/IP," in *Workshop on Multimedia Security at ACM Multimedia '02*, 2002.

[85] D. Kundur and K. Ashan, "Practical Internet Steganography: Data Hiding in IP," 2002.

[86] C. E. Shannon, "A Mathematical Theory of Communication," Bell Systems Technical Journal, 1948.

[87] S. Wendzel. (2007, Nov.) Doomed Reality. [Online]. http://files.doomed-reality.org/Papers/protocolhopping.txt, accessed April 2008.

[88] E. Bertino, B. Catania, and E. Ferrari, "A Nested Transaction Model for Multilevel Secure Database Management Systems," in , vol. 4, 2001, pp. 321-370.

[89] D. Alman, "HTTP Tunnels Through Proxies," 2003.

[90] J. S. Thyer and R. Wanner, "Covert Data Storage Channel Using IP Packet Headers," 2008.

[91] S. Zander, G. Armitage, and P. Branch, "A Survey of Covert Channels and Countermeasures in Computer Network Protocols," in , vol. 9, No. 3, 2007.

[92] R. A. Kemmerer and P. A. Porras, "Covert Flow Trees: A Technique for Identifying and Analyzing Covert Storage Channels," 1991.

[93] D. V. Forte, C. Maruti, M. R. Vetturi, and M. Zambelli, "SecSyslog: an Approach to Secure Logging Based on Covert Channels," in *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2005.

[94] R. A. Kemmerer, "Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels," ACM, 1983.

[95] J. Sarkesain and N. R. Howes, "Dynamic Virtual Communities and Mobile Agent Architecture," in *3rd Annual IEEE Information Assurance Conference*, Westpoint, 2002.

[96] Institute for Defense Analysis, *Cyber Operations and Information-Warfare System Users Manual*. December 2004.

[97] Joint Chiefs of Staff, "Joint Publication 3-13: Information Operations," 2006.

[98] J. F. Kennedy. (1960, Apr.) John F. Kennedy Presidential Library and Museum. http://www.jfklibrary.org/Historical+Resources/Archives/Reference+Desk/Speeches/JFK/JFK+Pre-Pres/1960/002PREPRES12SPEECHES_60APR22A.htm, accessed June 2008.

[99] L. Duboc, D. S. Rosenblum, and T. Wicks, "A Framework for Characterization and Analysis of Software System Scalability," 978-1-59593-811-4, 2007.

[100] C. G. Girling, "Covert Channels in LANs," 1987.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. John Sarkesain
   Ashburn, Virginia